Internet of Things Heterogeneous Interoperable Network Architecture Design

Bhalerao, Dipashree M.

Publication date:
2014

Document Version
Accepted author manuscript, peer reviewed version

Internet of Things Heterogeneous Interoperable Network Architecture Design

A DISSERTATION

SUBMITTED TO THE DEPARTMENT OF

ELECTRONICS ENGINEERING

OF

AALBORG UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

DIPASHREE MILIND BHALERAO

3rd Oct 2014

Supervisor:

Professor Ramjee Prasad, CTIF, Aalborg University, Denmark

Co-supervisors:

Assoc. Prof. Tahir Riaz, AAU, Aalborg University, Denmark

Professor Ole Brun Madsen, AAU, Aalborg University, Denmark

Professor U. B. Desai, IIT, Hyderabad, India

The Assessment Committee:

Associate Professor Reza Tadayoni (chairman), Aalborg University Copenhagen

Professor Marite Kirikova, Riga Technical University

Professor B.S. Chowdhry, Mehran University of Engineering & Technology, Jamshoro, Pakistan

Moderator:

Prof. xx, xx, xx

Date of Defence: 3rd Oct, 2014

ISSN: XXXX-XXXX

ISBN: 978-87-7152-084-2

Dedicated to my parents

Internet ting er (IoT) stade udlede, at der ikke er modne tingenes internet arkitektur til rådighed. Afhandlingen bidrager en abstrakt generisk tingenes internet henvisning arkitektur udvikling med specifikationerne. Nyheder i afhandling foreslås løsninger og implementeringer til skalerbarhed, heterogene interoperabilitet, sikkerhed og udvidelse af tingenes internet arkitektur for landdistrikter, fattige og katastrofale (RPC) områder. VLC er foreslået og bevist som en af de passende Internetwork betyder at overvinde ulemperne ved landdistrikter og katastrofale områder.

IVarious operationer eller funktionelle krav, af tingenes internet arkitektur bestemmes ved at finde detaljeret udførelse sekvens af operationer. Komplet tingenes internet software og hardware komponent topologi forklares med komponent og Udplaceringsdiagrammer hhv. IoT arkitektur begrænsninger eller ikke-funktionelle krav såsom specifikationer, skalerbarhed, sikkerhed og privatlivets fred, datamængder, enhed tilpasningsevne, interoperabilitet, strømforbrug, selvbevidsthed og søgemekanismer funktioner analyseres. Software arkitektur er udviklet ved hjælp af krav analyse af funktionelle og ikke-funktionelle krav. Abstrakt tingenes internet arkitektur model er valideret ved brug af Arduino single-board microcontroller, til overvågning af lysintensiteten ved hjælp af LDR.

.Som et første ikke funktionelt træk skalerbarhed arkitektur overvejes. Nogle af IoT-applikationer (alle sensorer baseret) sende de samme oplysninger flere gange eller inden for et bestemt område af værdier. Det er bevist, at reduktionen af data på en kilde, vil resultere i enorme lodrette skalerbarhed og indirekte horisontal også.

Anden ikke funktionelt træk bidrager i heterogene interoperable netværk arkitektur for begrænsede Ting. For at eliminere stigende antal gateways, Wi-Fi-adgangspunkt med Bluetooth, ZigBee (nyt adgangspunkt er indkaldt som BZ-Fi) foreslås. Sameksistens af Wi-Fi, Bluetooth og Zigbee netværk teknologier resulterer i interferens. For at reducere interferens, der Orthogonal Frequency Division Multiplexing (OFDM) foreslås gennemført i Bluetooth og Zigbee. Det foreslåede netværk arkitektur gør det muligt at rejse og til at kommunikere Bluetooth og Zigbee knudepunkter i Wi-Fi-netværk uden Wi-Fi-interfacet i dem.

Tredje ikke funktionel funktion finder sikkerhedsarkitektur for alle typer af grå huller angreb (DoS attack). Den foreslåede arkitektur er baseret på algoritme designet netværkslagprotokol. Resultaterne bekræfter nær omkring 100% opsving i pakken drop rate. Det unikke ved

algoritmen er i tre stikprøver, hvis gennemførelse afgørelse træffes under kørslen, sammen med den første kontrol for et fast antal gange.

IVLC overvinder spørgsmål af langdistance dækning, driftsomkostninger, gentagne investeringer i den katastrofale område og en hurtig forbindelse, kan overvindes ved hjælp af handy cam for en lang distance (snesevis af KMs forventet) udendørs kommunikation. Eksperimenter er gjort for forskellige hastigheder og på forskellige tidspunkter.

Række udfordringer og spørgsmål af tingenes internet arkitektur diskuteres i detaljer, for fremtidig forskning.

Abstract

Internet of Thing's (IoT) state of the art deduce that there is no mature Internet of Things architecture available. Thesis contributes an abstract generic IoT system reference architecture development with specifications. Novelties of thesis are proposed solutions and implementations for Scalability, heterogeneous interoperability, security and extension of IoT architecture for rural, poor and catastrophic (RPC) areas. VLC is proposed and proved as one of the suitable internetwork means to overcome drawbacks of rural and catastrophic areas.

Various operations or functional requirements, of IoT architecture are determined by finding detailed execution sequence of operations. Complete IoT system's software and hardware component topology is explained with component and deployment diagrams respectively. IoT architecture constraints or non-functional requirements such as specifications, scalability, security and privacy, data volumes, device adaptability, interoperability, power consumption, self awareness, and discovery mechanisms features are analyzed. Software architecture is developed using requirement analysis, of functional and non functional requirements. Abstract IoT architecture model is validated using Arduino single-board microcontroller, for monitoring light intensity using LDR.

As a first non functional feature scalability of architecture is considered. Some of the IoT applications (all sensors based) send the same information repeatedly or within a specific range of values. It is proved that reduction of data at a source will result in huge vertical scalability and indirectly horizontal also.

Second non functional feature contributes in heterogeneous interoperable network architecture for constrained Things. To eliminate increasing number of gateways, Wi-Fi access point with Bluetooth, Zigbee (new access point is called as BZ-Fi) is proposed. Co-existence of Wi-Fi, Bluetooth, and Zigbee network technologies results in interference. To reduce the interference, orthogonal frequency division multiplexing (OFDM) is proposed to be implemented in Bluetooth and Zigbee. The proposed network architecture allows to travel and to communicate the Bluetooth and Zigbee nodes in the Wi-Fi network without Wi-Fi interface in them.

Third non functional feature finds security architecture for all types of grey holes attacks (DoS attack). The proposed architecture is based on algorithm of designed network layer protocol. The results verifies near about 100% recovery in the packet drop rate. The

uniqueness of the algorithm is in three random tests, whose implementation decision is taken at run time, along with the first checking for a fixed number of times.

It is shown that the famous Okumura–Hata model is insufficient for defining all ICT areas**.** A new ICT area model is proposed for rural, poor and catastrophic (applicable for any area) areas. These definitions help in understanding development of required area from ICT point of view.

VLC overcomes issues of long distance coverage, operating cost, repeated investments in the catastrophic area and a fast network connection, can be overcome by using handy cam for a long distance (tens of KMs expected) outdoor communication. Experimentation is done for various speeds and at various times.

Number of challenges and issues of IoT architecture are discussed in detail, for future research.

Acknowledgements

I take this opportunity to express my profound gratitude and deep regards to Prof. M. N. Navale, the founder president and Mrs. Sunanda M.Navale, the secretary of Sinhgad Technical Education Society (STES), who gave me the opportunity of persuing PhD at Aalborg, Denmark.

I take this opportunity to express a deep sense of gratitude to Prof. Ramjee Prasad Director and professor CTIF, Aalborg University for his motivating, affectionate, and professional guidance at every stage of the PhD work.

Special thanks to Head of Department, Prof. Borge Lindberg for his valuable technical support in the PhD journey. I thank to PhD school for their valuable feedbacks, guidance and support.

I would like to express the deepest appreciation to Prof. Sandeep Inamdar, who made the STES and Alborg University tie up possible by providing the kind, and prompt support right from the beginning to the end of the PhD journey.

Many thanks to Prof. Ole Brun Madsen for his support and guidance provided to me with his subject expertise, without, which, it was difficult to complete the PhD work. I am very much grateful to Dr. Tahir Riaz, who has guided me at all the steps of PhD technically and non-technically. I would like to thank Prof.U.B.Desai Director, Hydrabad, India for providing his guidance. Technical discussions and feedbacks of my research work along with Prof. Ramjee, Prof.Ole, and Dr.Tahir Riaz have helped me to improve my research work.

I would like to thank Prof. Neeli Rashmee prasad for her technical support and Mrs.Jyoti Prasad who has made our stay possible at Denmark with love and affection at all the times.

I am obliged to Jens Eric Petersen, Dorthe Sparre, Susanne Nrrevang, and Inga Hauge for the valuable information provided by them in their respective fields. I am grateful for their cooperation during the period of my assignment.

Special thanks to almighty, my parents, husband, brother, sisters and daughter for their constant encouragement without which this accomplishment would not be possible.

I would like to thank all those whose names are not in the above list, but they have supported me in this PhD research.

Table of Content

Chapter – 4 - Design Of Heterogeneous Interoperable IoT Network Architecture

Chapter -5 - Security Architecture design for all Types of Black and Grey Holes

List of Tables

Mandatory Page

1. **Thesis title** - Internet of Things Heterogeneous Interoperable Network Architecture Design

2. **Name of PhD student** - Dipashree Milind Bhalerao

3. **Name and title of supervisor and any other supervisors**

Supervisor:

Professor Ramjee Prasad, CTIF, Aalborg University, Denmark

Co-supervisors:

Assoc.Prof. Tahir Riaz, AAU, Aalborg University, Denmark

Professor Ole Brun Madsen, AAU, Aalborg University, Denmark

Professor U. B. Desai, IIT, Hyderabad, India

4. **List of published papers:**

Paper 1: Dipashree M. Bhalerao, M. Tahir Riaz, Ole Brun Madsen, Ramjee Prasad "An Internet of Things Generic Reference Architecture" IoT journal, 2160-2271, Pages Nos.25-39, March 2013, NewWorldPublishers.

Paper 2: Dipashree M. Bhalerao, M. Tahir Riaz, Ole Brun Madsen, Ramjee Prasad "IoT Heterogeneous Interoperable Network Architecture Design using ZB-Fi Access Point" IoT journal Accepted, NewWorldPublishers

Paper 3: Dipashree M. Bhalerao, M. Tahir Riaz, Ole Brun Madsen, Ramjee Prasad "Scalability in IoT Architecture" Internet of Things, 3rd International Conference for Industry and Academia, IEEE-M2M, WUXI, China, ISBN: 978-1-4673-1345-2, Pages: 372 – 376, 2012

Paper 4: Dipashree M. Bhalerao, M. Tahir Riaz, Ole Brun Madsen, Ramjee Prasad "On A New Global Catastrophic ICT Model", Publication Year: 2011 Advanced Communication Technology (ICACT), 2011 13th International Conference on, 978-1-4244-8830-8, Page(s): 1064 – 1068

Paper 5: Dipashree M. Bhalerao, M. Tahir Riaz, Ole Brun Madsen, Ramjee Prasad "Rural, poor and catastrophic ICT area standardization and modelling", Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on , IEEE CONFERENCE PUBLICATIONS, ISBN 978-1-4673-4533-0, Publication Year: 2012 ,Page(s): 103 – 107,

Paper 6: Dipashree M. Bhalerao, M. Tahir Riaz, Ole Brun Madsen, Ramjee Prasad "On the Use of the Universal Okumura-Hata Model" Second International Multi Topic Conference, IMTIC 2012,Emerging Trends and Applications in Information Communication Technologies, © Springer-Verlag Berlin Heidelberg 2012, ISBN: 978-3-642-28961-3, March 28-30, 2012 pages- 154–163

"This thesis has been submitted for assessment in partial fulfilment of the PhD degree. The thesis is based on the submitted or published scientific papers which are listed above. Parts of the papers are used directly or indirectly in the extended summary of the thesis. As part of the assessment, co-author statements have been made available to the assessment com mittee and are also available at the Faculty. The thesis is not in its present form acceptable for open publication but only in limited and closed circulation as copyright may not be ensured."

Chapter 1

Introduction

1 Motivation

After the World Wide Web and mobile Internet technologies, the time has come for the Internet of Things (IoT). IoT is an internetwork meant to monitor or control valuable things of human, society and industry. Requirement of monitoring or controlling Thing is nothing but an IoT application. The motivation is revealed by the benefits society is going to get because of IoT. So, the next few lines explain the important benefits the society and the environment will get. Data monitoring and controlling is required at any time, from any place, and by anyone. Environmental, societal, and industrial applications may require monitoring or controlling data. This monitoring can be done without any efforts and waste of time. Agriculture, medical services, weather monitoring, and in any other application data can be monitored, controlled, for better conditions. Tasks, sometimes beyond human understanding or capacities can be done with IoT e.g. detection of a catastrophe, or problems in the soil for a crop etc. The accuracy of information will be better as compared to a human being. Tracking and tracing of Thing related data assist in understanding the following facts.

1. To monitor data, at anytime from any place (where human can't go), and by anyone quickly, economically, and smartly.
2. Decision-making becomes easier by knowing all the related information of the application.
3. To prevent the worst conditions by getting information in time or before occurrence of a catastrophe (atmospheric or manmade). Information can save the lives of many people and the destruction in all respects.
4. To understand the efforts required or to reach a required threshold value.
5. To secure data on internetwork.
6. To assist in development of rural, poor areas.

All the above tasks in a day to day activity can be made possible because of hundreds of thousands of IoT applications. As each application has various requirements, it is interesting to design the abstract generic reference architecture, which will cover features such as scalability, heterogeneous interoperability, security, and development of rural, poor and catastrophic (RPC) areas. Further, RPC area developments can be understood by defining them from the ICT point of view. Looking at the benefits mentioned above, the research topic is finalized.

1.2 Challenges

At present there is no mature standardized IoT architecture available. The architecture design is vast, as the functional and the non functional perspectives themselves are huge domains, increasing the complexity of the design. We have worked for scalability, heterogeneous interoperability, security architectures and area development along with abstract system reference architecture. The challenge is to design and validate an abstract generic IoT system reference architecture with a solution for each of the above four perspectives, which will contribute in practice.

Providing a solution for heterogeneous interoperability of Things with Wi-Fi, Bluetooth, and Zigbee co-existence, and achieving heterogeneous interoperability (HI) along with the minimum interference using OFDM, are few other considerable challenges.

Co-operative grey hole detection is one of the challenges of security. A solution reinforces security architecture with the denial of a service attack (to some extent) at the network layer.

Research becomes horizontal instead of vertical, which creates a challenge of understanding of totally different topics and design architecture.

1.3 Background

Electronic Product Code (EPC) global architecture is the basic inspiring architecture for the Internet of Things architecture. The EPC global Network is a set of technologies that enable immediate, automatic identification and the sharing of information on items in the supply chain. In this way, the EPC global network makes organizations more effective by enabling the true visibility of information about the items in the supply chain. The EPC global network is a closed loop chain. The IoT has a vision of ubiquitous networking with mobile and fixed communication. IoT architecture shall be the exploitation of the EPC global network architecture with a web service and the Grid service concepts, the Service Oriented Architecture (SOE), Unique Item Identifier (UII) concepts, and a namespace resolver to accommodate legacy coding schemes for identification (incl. EPC and URL), and viewing the needs for governance, Quality of Services (QoS), security, privacy, and other socio-economic issues, and edge technologies (RFID, SENSORs etc.).

Edge Technologies shall convey information such as location, time, and state. In terms of RFID, for IoT it will have RFIDs with computation and communication capabilities embedded in it, which is not there for the EPC global network. Other various features for IoT can be multi-level tagging (objects/device/persons/locations) with RFID and other Automatic identification and data capture (AIDC) technologies, and automated events to trigger data

communication / transactions: i.e. self ID of interconnected and ubiquitous computing objects/ devices, pervasive computing, and network environments for device to device communication, and extended data/communications and standard structures that are similar to GS1/EPC global standards. For instance: extended EPCIS standards for understanding more complex data elements than the What, Where, When, and Why events occurring in any supply chain. The state of the art says that the Internet of things technology is in the developing stage and so is its architecture.

1.4 Research Goals

1. The primary goal of the thesis is to design generic reference system architecture for the Internet of Things. This architecture shall be competent for physical Things. The design has the following steps.
    a. To design Abstract Generic IoT System Reference Architecture with steps
        i. Requirement analysis of functional and non functional features.
        ii. To design and validate Abstract IoT Model.
        iii. To design Abstract IoT system reference architecture.
2. To contribute in scalability as a non functional architecture feature.
3. To provide a solution for heterogeneous interoperable network architecture (along with the co-existence of Wi-Fi, Bluetooth, and Zigbee) for constrained device's as a non functional architecture feature.
4. To contribute IoT architecture from the security architecture perspective, by formulating the detection mechanism for all types of co-operative grey hole, and reduce the packet drop ratio to zero.
5. To define a rural, poor, and catastrophic areas from the ICT point of view, to search RPC area requirements for IoT architecture design.
6. To fix up the communication technology for RPC area.

1.5 Research Methodology

Research methodology used is Define – Measure – Analyze – Design – Verify (DMADV). Each respective chapter has all five steps.

Define – Precisely defining the IoT architecture requirements.

M – Measuring the state of art for IoT architecture requirements and shortcomings for scalability, HI,security, IoT RPC architecture.

A – Analyzing and determining the root causes of the shortcomings for each.

D – Design the architecture / scheme/ protocol / algorithm to meet the problem.

V – Verify the design performance to meet the challenges.

Simulations, actual experimentations and theoretical presentations are used for verification . Ns2 simulator is used for proving IoT architecture scalability in chapter three, all types of grey holes attack detection algorithm in chapter five and for plotting QoS plots in chapter 6. Abstract IoT model is validated using Arduino platform in chapter three. VLC suitability is proved using handy cam as a receiver and transmitter which is self designed and implemented with PIC micro-controller based transmitter.

1.6 Novelties and Scientific Original Contributions

1. The research contributes in the design of abstract IoT system reference architecture. Validation with actual experimentation of abstract IoT model is carried out with Arduino. It extends further to the scalable IoT reference architecture. The common solution for the scalability for any architecture is proposed and proved practically.
2. A heterogeneous interoperable IoT network architecture is put forward for the co-existence of Wi-Fi, Bluetooth, and Zigbee technologies. The proposed solution manipulates the Orthogonal Frequency Division Multiplexing (OFDM) in the Zigbee and the Bluetooth network architecture theoretically.
3. An algorithm is proposed and proved for detecting all types of grey hole attacks. A novelty is of three random tests in the algorithm, which makes it difficult for the attacker to introduce a grey hole attack in the network.
4. The Okumura – Hata model is insufficient for defining all the areas. A new ICT area model is proposed and proved.

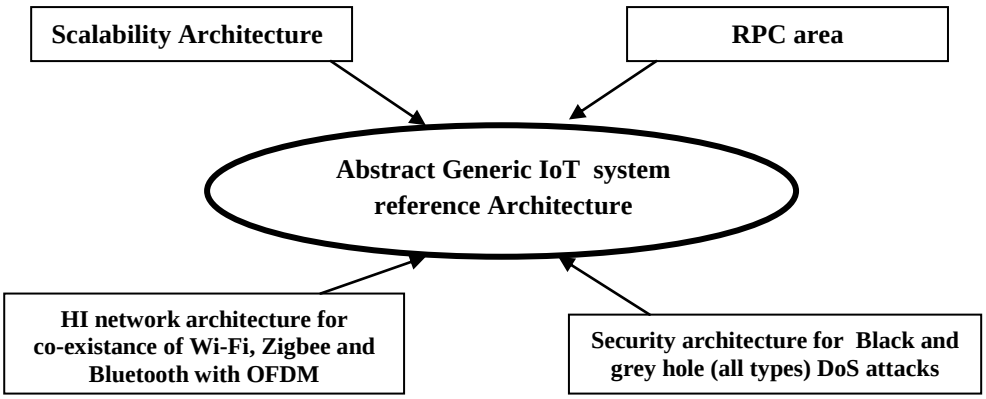


Fig 1-1: Architecture features covered in the Thesis.

1.7 Thesis organization

The state of the art of IoT architecture can be clearly understood in chapter two. The European commission has funded many IoT projects. These projects provide the best overview of the state of the art of the IoT architecture, IoT modelling, communication protocols, identification and resolution frameworks, object platforms, and security. The thesis main focus is on architecture's state of the art.

An abstract generic IoT system reference architecture has been proposed in Chapter three. Arduino based remote monitoring of light dependent resister (LDR), proves the core IoT architecture. In the same chapter, it is revealed that the scalability of IoT architecture can be achieved from every small thread to processes, and arrangements of components or packages. It is proposed and proved that by dispatching values as an encoded single byte and decoding it in the business process will support in decreasing the scalability of power consumption, data storage at the server side, and vertical handoff time and traffic congestion will be scaled down. The scalability achieved will be at each block from the source (Thing) to the server, and from the server to the user. It will indirectly assist in scaling the complete IoT architecture. Proposed solution is straightforward but the effect will be tremendous. The proposed logic takes care of the security as a derivative of it.

Chapter four proposes the HI network architecture for the co-existence of three networks as Wi-Fi, Bluetooth and Zigbee. Chapter divulges solution for HI, co-existence interference with the proposed BZ- Fi access point. Design of network layers and the required network protocol stacks for the Bluetooth and Zigbee with the OFDM are explained in the next few sections.

The security algorithm is proposed in chapter five for scalable network of Things e.g. mobile ADHOC networks. The chapter focuses on a huge IoT security framework. A network layer protocol for black and grey hole co-operative attacks is proposed and proved. Chapter presents an algorithm, the pseudo code and the NS2 results for the same. The proposed and existing algorithm comparison with respect to packet drop ratio is provided with analysis. From the above analysis, the security architecture for the grey hole (DoS) attack is designed.

Chapter six and chapter seven carry out research for IoT architecture design for rural, poor and catastrophic areas. Chapter six invents an information and communication technology (ICT) definitions of rural, poor, and catastrophic areas. The research will be applicable for designing IoT (or any other architecture) architecture for a rural, poor, and catastrophic areas and demonstrates that the famous Okumura-Hata model is not sufficient for area definition,

but along with it, the QoS behaviour pattern of a network is also required. Simulations are performed for the scenarios of a catastrophic area, rural area, and poor area. The QoS behavioural pattern available from simulations is utilized to define all these areas. The mathematical model for the same QoS parameters is developed. It is also highlighted that standardizing these definitions in a developed and a developing countries is very much important. ICT area definitions revels a clear picture of the existing facts, scope for further development, possible investments, drawbacks, and other things in that area for information and communication technology.

Chapter seven presents the experimentation results with easily available handy cam for the on off keying (OOK) method of VLC for a long distance outdoor scenario. VLC can be exploited for remote, rural, and catastrophic areas as a first aid communication means for ubiquitous connectivity.

Chapter eight ends the thesis with conclusions and future work. Each research chapter of thesis came to specific conclusions with reasons. This chapter gathers conclusions on end results of chapter's two to seven. Future work constitutes suggesting ideas which are directions for researchers.

1.8 Correlation of Thesis Chapters

Chapter two exhibit state of the art of various features for IoT architecture design. It presents the complete picture of issues, challenges present, discussions and analysis done on it. Chapter 6 discusses requirements for RPC area development from ICT point of view. Chapter seven endeavours on the connectivity problem in RC areas, which is one of the internet types and is discussed in chapter six. Chapter two and six enrich requirements for IoT generic architecture design in almost all aspects. Chapter three proposes Abstract Generic IoT System Architecture using chapter two, four, five, six and seven as a base.

Chapter three further assists on scalability which is one of the non functional features of IoT architecture. Chapter four and five foster on Heterogeneous Interoperability and security architectures as a second and third non functional features of IoT architecture.

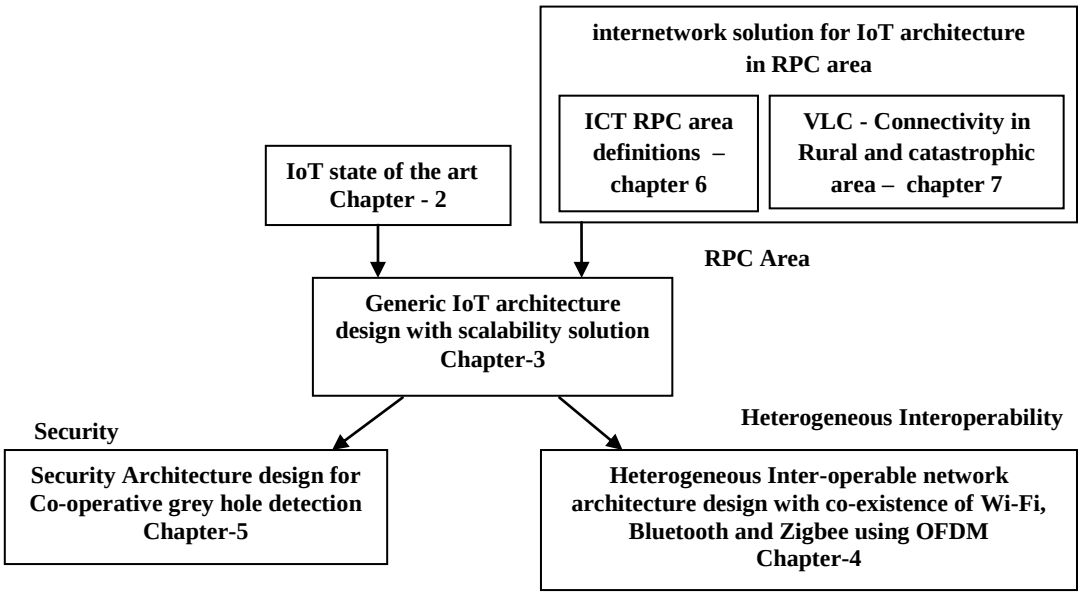


Fig 1-2: chapter's correlation flow diagram

Refer Fig. 1-2 for understanding thesis chapter's corelation.

1.9 Important References used in Thesis

[1] CERP-IoT, Cluster of European Research Projects on the Internet of Things, Vision and challenges for realizing the internet of things, Edited By, Herald Sundmaeker, Patrick Guillemin, PeterFriess, Sylvie Woelffle , 2011

[2] Internet of Things - Architecture, ―SOTA report on existing integration frameworks/architectures for WSN, RFID and other emerging IoT related technologies – wrt to requirements, IoT-A Internal Report, IR1.2, December 2010.

[3] Adam Dunkels. Programming Memory-Constrained Networked Embedded Systems. PhD thesis, Swedish Institute of Computer Science, February 2007

[4] Adam Dunkels. Full TCP/IP for 8 Bit Architectures. In Proceedings of the First ACM/Usenix International Conference on Mobile Systems, Applications and Services (MobiSys 2003), San Francisco, May 2003

[5] Rong Chai; Wei-Guang Zhou; Qian-Bin Chen; Lun Tang "A survey on vertical handoff decision for heterogeneous wireless networks" Information, Computing and elecommunication, 2009. YC-ICT '09. IEEE Youth Conference on Digital Object Identifier:,10.1109/YCICT.2009.5382368 Publication Year: 2009 , Page(s): 279 – 282

[6] Zacharias, S. Newe, T. O'Keeffe, S. Lewis, E. ITS Telecommunications (ITST), 2012 12th International Conference on, Digital Object Identifier: 10.1109/ITST.2012.6425289, Publication Year: 2012 , Page(s): 785 – 790

Garroppo, Rosario G "Experimental assessment of the coexistence of Wi-Fi, ZigBee, and Bluetooth devices" , World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a, 20-24 June 2011, Page(s): 1 - 9

[7] M. Howlader, C.J. Kiger and P.D. Ewing "Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Facility Environment" Division of Fuel, Engineering and Radiological Research, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, July 2007

[8] Axel Sikora, Voicu F. Groza "Coexistence of IEEE802.15.4 with other Systems in the 2.4 GHz-ISM-Band", in Proc. IEEE Instrumentation & Measurement Technology Conference, Ottawa, May 2005, pp.1786-1791.

[9] Texas Instruments Product Bulletin (2003), Wireless performance optimization solutions:Bluetooth and 802.11 co-existence. http://focus.ti.com/pdfs/vf/wireless/co-existencebulletin.pdf

[10] Digital equipment corporation maunard, Massachusetts DECnet, " DIGITAL Network Architecture , (Phase IV)"

[11] Glenford E. Mapp, FatemaShaikh, David Cottingham, Jon Crowcrof "Y-Comm: A Global Architecture for HeterogeneousNetworking "Invited Paper, WICON '07: Proceedings of the 3rd international conference on Wireless internet , October 2007

[12] JaydipSen, SripadKoilakonda, ArijitUkil "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks " Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on Publication Year: 2011 , Page(s): 338 – 343

Chapter 2

IoT

State of the Art

2.1 Introduction

Various IoT architectures are proposed by individual researchers, academicians, and companies from various countries. As the research continued further, the IoT definition started taking shape of a more mature level. Various definitions are available with different aspects and meanings of IoT, and will be discussed in the chapter. All definitions don't have the same meaning and lack in defining the architectures. Section one analyzes these definitions to understand various aspects of IoT. This helps in finding out missing parts of the architecture. Section one outlines the chapter flow diagram (Ref. Fig2.1).

The state of the art covered in this chapter is focused on architecture, and various parts of architecture like protocols, security, Identification and Resolution Frameworks, IoT object platforms and IoT modelling techniques. Each and every part is discussed in detail on the basis of individual research papers, survey papers, public projects, commercial projects, and finally the standardization bodies' survey.

Various survey papers and other research papers findings related to IoT architecture are analyzed in section 2.2 to understand behaviours, qualities, issues and challenges in IoT's various applications. In a continuation of survey papers, the European Lighthouse Integrated Project (IoT-A) is also analyzed. A comparison with IoT-A and a state of the art found by our analysis is studied, based on the development of concrete generic IoT architecture. Public projects, standardization, and EU projects are analyzed based on features like scalability, device adaptability, service oriented architecture, interoperability, security and privacy, power consumption, data volumes, and discovery mechanisms. IoT-A is working out the basic requirements for IoT architecture. It is specified that some facts are missing in IoT-A.

Analysis of the different protocols from single mode to the web communication is done in section 2.3. Section further analyzes all the possible networking technologies, which could be suitable for IoT communication. Network architecture state of the art for IoT is put up in section 2.4. Network architecture shall take into account computing power and memory features so as to adopt the TCP/IP protocol accordingly. Things are dynamic and static in nature. Accordingly, changes will be there, in the network architecture of both. Most of the papers have suggested three layer architecture with application, network and a perception layer. Few have suggested it with five layers having business, application, processing, transport, and a perception layer.

State of the art of security covers fixed and unfixed attacks for peripheral networks in section 2.5. Section 2.6 covers the state of the art of identification and resolution

frameworks, which provides the available address and identification techniques. Standardization activities in identification are also put for a better understanding of the topic. State of the art on IoT objects platforms covered in section 2.7 discusses hardware features and OS requirements. Various modelling tools and techniques that are required for application development are also discussed with projects in section 2.8. The available modelling tools are not sufficient for modelling and changes are required. The new changes, requirements in these tools are discussed in relation with some applications. Issues and challenges in IoT, open a big umbrella for many areas of research, from all disciplines in section 2.9. Section 2.10 concludes the chapter.

Section 2.1.1 definition analysis (table 2-I) contributes in understanding the vision of the IoT architecture easily. Section 2.2 all tables (analysis of existing architectures, recommendations, comments on them) and analysis contributes in giving our definition of IoT. Features are summarized along with new requirements of all sections in tabular format, so that readers cover all points at a glance, for the respective state of the art. Analysis at the end of all sections is contribution of the chapter. Figure 2.1 is the logical flow of the chapter as per the analysis of the main parts of the chapter.

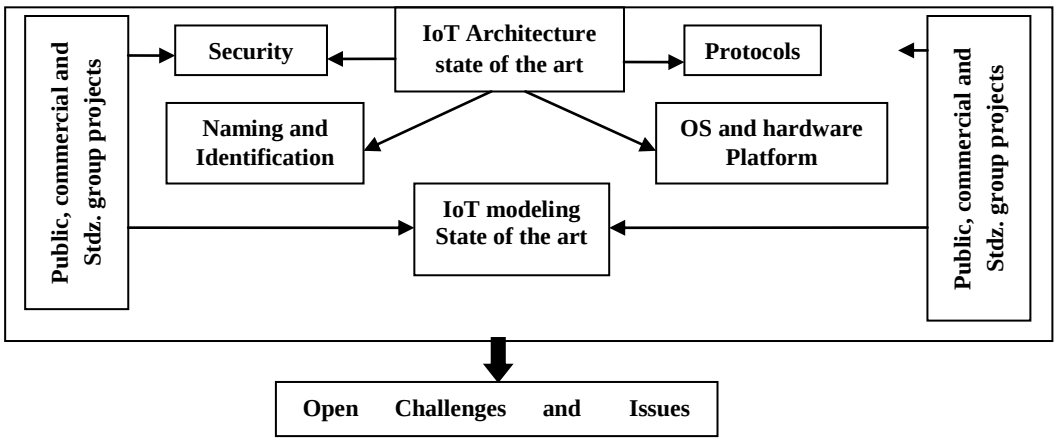


Fig. 2.1: Chapter Flow Diagram

Chapter is very much beneficial for IoT researchers. Section 2.3 to 2.8 discusses some of the features in detail. Section 2.9 provides research topics in all IoT domains. Chapter connotes to state of the art of IoT. The major contributions are IoT definition, specifically finding imperfections and deficiencies in IoT architecture and other linked features of it.

2.1.1. IoT Definitions

There are several definitions that exist for IoT. Many of them have evolved over time due to the emergence of new technologies and an improvement in the existing technologies. Unless and until, the basic IoT methodologies are clear, core IoT architecture cannot be developed.

Generic architecture is built up on core architecture. Efforts should be made to develop the generic architecture. Various IoT definitions are discussed and summarized below. At the end we conclude with our suggestions.

The terminology "Internet of Things" was presented first time by Ashton in 1998, as RFID tags connected to objects for storing, and using object's information on the internet (closed loops) in supply chains. The focus was only on RFID connected objects. Here, RFID is using radio frequency to connect an object to the internet trough wireless or wired networks. Definition has a limitation on the meaning of objects. According to it objects connected by RFID can only be called as Things. EPC global is based on the same definition and concept.
Around **2003-04, the concept of Internet 0 [1]** came forward. It says that everyday objects, can be connected to the Internet. This gave rise to concepts of heterogeneous devices and connectivity to narrow waist TCP/IP protocols for achieving the same. Definition has expanded the object concept covering the real physical world in to objects. As per application requirements, an object can be connected to RFID, NFC, actuators, or other heterogeneous devices for Internet connectivity. These devices are normally constrained devices. Constraints are in memory, computing power, and communication range. These constraints reflect the requirement for connecting constrained devices to the Internet with TCP/IP. Looking at the object definition many meanings are hidden, which are not explored here. Definition tries to complete the vision of anything that can be connected to the Internet to some extent.

CASAGRAS, 2009 definition [2] *"A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes the existing and evolving Internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterized by a high degree of autonomous data capture, event transfer, network connectivity, and interoperability"*

Object meaning is expanded to virtual from physical. Considering the huge number of physical and virtual objects, automatically many questions come into the picture as, many things can be connected to the Internet and how? What are the technologies for connecting them to the Internet? How huge data will be collected, stored, and transmitted. What services can be offered with this database, or with Things? Is this service handled by an individual object or in a cooperative way? If each of the objects offers some information, what will be the service related to it? To ask for this service further, how is the user going to call for a specific object? For answering these questions object identification technology is required.

Heterogeneous devices lead to heterogeneous data, services, and heterogeneous interoperability of devices. Any change in the state of an object shall be communicated as an event and accordingly further action can be decided.

Naturally, for accommodating these new changes the existing Internet is not sufficient and hence, new changes are expected in the architecture of the Internet. Each and every part of the network plays a role in this communication. This makes infrastructure as a basic component of the IoT.

Even if the definition says virtual and physical objects, standardization comes into the picture further, which may not allow all objects to become part of IoT. There is no mention of privacy and security, when such a huge data is collected.

SAP definition [3] *"A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these 'smart objects' over the Internet, query, and change their state and any information associated with them, taking into account security and privacy issues."*

Definition keeps main focus on physical objects, smart objects, and active objects and they are treated as participants of the information network of IoT, to disseminate information as per queries, and can change the state. I.e. device to device communication is possible. Virtual things are not taken into consideration. Various types of services can be made available with such information. The information network focuses on service related to devices, data, and discovery etc.

Future Internet Assembly/Real World Internet definition [4]- "*The IoT concept was initially based around enabling technologies such as Radio Frequency Identification (RFID) or wireless sensor and actuator networks (WSAN), but nowadays spawns a wide variety of devices with different computing and communication capabilities – generically termed networked embedded devices (NED). […] More recent ideas have driven the IoT towards an all encompassing vision to integrate the real world into the Internet […]"*

Definition provides support to physical objects of the Internet along with the entire real world thing. These devices can compute and communicate. But it is possible to connect also objects, which don't have computing power or RFIDs. The best example can be virtual things.

EPoSS definition [5] focuses on Things with intelligence, unique address based on standard protocol, and having virtual identity. They can communicate with social, environmental, and user contexts. Virtual Things widens the scope of objects / Things. It connects almost everything to the Internet as physical as well as virtual objects.

We can take abstract meaning as a vision to connect objects or smart objects to the Internet for monitoring, controlling, and managing information. All the above definitions are not taking into account or mentioning limitations of connections because of various types of objects. In a broad vision IoT is a network for connecting users/devices through digital means with only physical objects or humans to each other. All the above definitions focus on object types, network, its infrastructure, services, and then on other features in various extents. We conclude that no, one definition is complete. Various concepts of IoT from different definitions can be combined together to create a more logical and complete IoT definition, which focuses on any Thing (not only human, physical, virtual) from anyplace, which can communicate to any other Thing (not only human, physical, virtual) in the true sense.

Table2-I: IoT Definition Analysis

Defined By	Object	Network	Services	Other features
Ashton	Only RFIDs	Closed private internet	Supply chains	Nil
Internet 0	Heterogeneous physical constrained objects. e.g. RFID, NFC, actuators, etc	Internetwork,	Data capture, operations with data base	narrow waist TCP/IP
CASAGRAS	physical and virtual objects	Global legacy. Internet and new evolving network and its infrastructure.	Autonomous Data capture, event transfer, HI, co-operative and normal communication.	Object identification, cooperative services.
SAP	physical smart objects	information network or SOA	Device to device communication.	Security, privacy, services related with data as query, update, delete etc.
Future Internet Assembly/Real World Internet definition	Smart objects, physical all the real objects in the world.	Internet.	Normal communication.	Computing capabilities.
EPoSS	Smart physical and virtual objects.	Internet	Device to device, normal communication.	Unique address

Table 2-I summarizes the various features covered in all the definitions. Different concepts can be defined in an abstract manner. We can say that object types, networks, services, and other special concepts can be combined together. When we say any concept, everything related with it becomes a part of definition. We contribute our IoT definition after studying all the generic architecture requirements, in analysis part.

2.2. State of the Art on IoT Architecture

Electronic product code (EPC) global architecture [6] is the base for Internet of Things architecture. Paper [7] works on the EPC network architecture for pervasive and ubiquitous RFID and sensor node applications. Electronic product code (EPC) global architecture is the basic inspiring architecture for the Internet of Things architecture. Detailed background about EPC is covered in chapter 1.3.

There are many survey papers available to date. Each has a different direction of survey. These papers focus on various IoT visions, issues, and challenges and have covered state of the art to a very small extent. Survey paper [8] provides visions of IoT, various enabling technologies for it, benefits of its use, various applications, and major research issues. Thing, Internet and semantic oriented visions or indirectly various meaning, definitions of IoT are discussed very nicely and in detail in the paper. There is a big number of IoT enabling technologies from architecture to nano technology, but only identification, sensing and communication technology, and middleware are discussed. RFID, WSN, and RSN and their types are considered as basic objects. Middleware is software oriented architecture. Its advantages are discussed in detail.

Paper [9] presents a survey of technologies, applications, and research challenges for IoT. Heterogeneous interoperability of device and data, self adaptation, security, energy optimization techniques, and mobile technologies are discussed. The application list of most of the survey papers is mostly related to controlling and monitoring in the industrial, societal, and environmental domains. Computing, communication and identification technology, security, privacy, trust, distributed architectures, and their challenges are discussed in detail. The application list is also limited. Paper two and three are applicable for limited technologies and does not cover all technologies. The papers do not discuss projects in depth for mentioned technologies. All drawbacks of the previous papers are overcome in the European commission research road map [10]. It explains in detail the visions, applications, technologies, completed projects, issues, and challenges. This document has covered almost everything related with IoT. The roadmap starts from scratch with the various definitions of IoT, and properties of Thing or objects. As per application domains a detailed list of the possible applications is listed. It is stated that for enabling IoT, many technologies come into the picture. More or less, ten major technologies are discussed. It also delivers the research roadmap for IoT development. The document renders completed projects, sponsored projects, and lessons learned. It also briefs about the standardization efforts taken by the various bodies and its status.

The data analytic perspective of IoT [11] covers issues and challenges of data about searching and managing. It briefs about IoT visions (same as paper [2] above), applications (same as paper [2-3]), technologies, cleaning of data, semantic sensor web, data management in web, discovery, privacy and security, in data sharing and management are the main areas of discussion of this chapter. Technologies, issues and open challenges related with data are the main focus of the chapter.

IoT covers almost all the applications required in day to day life. Each application has different requirements in it. Various IoT architectures are presented by individual researchers, companies, and academicians from various countries. Architectures are proposed based on Service oriented architecture (SOA), Web of Things architecture, QoS architecture, Architecture imitating brain-neural systems of living organisms, extension of electronic product code (EPC) global standards architecture and many more. Service discovery [12-13], plug and play features and their integrated testing with challenges for SOA are rendered in the paper. Web of things [14-15] architecture proposes various prototypes for sensor nodes, and energy monitoring systems using the World Wide Web based on the RESTful approach. Paper [16] proposes the QoS architecture for IoT by controlling the transfer and translation requirement mechanisms in the three layered network architecture. The paper has further suggested cross layer QoS management facility and brokers residing in the lower layers.

IoT-A [17] project provides a detailed analysis of architecture with the help of public, commercial, and standardization bodies. It also focuses on IoT protocols, IoT modelling techniques, identity management framework, and security in detail.

IoT-A explains what is the architecture structure, how information is treated, distributed, and accessed, and the re-usability of the blocks for building higher level components. A meaningful exchange of information as per the queries requires proper categorization of data. Interoperability explains how much architecture is dependent on a specific technology. Reactivity to any changes is checked for adaptation. An analysis of all public projects tells that all features are not applicable for IoT implementation. Features are applicable to IoT at various levels.

It is observed that IoT-A has not analyzed individual IoT architecture research paper contributions much, which are giving various important directions for architecture.

IoT-A covers work of many standardization bodies, which are working on various activities of IoT. ETSI is working on M2M communications, ITU-T USN (ubiquitous Sensor Networks) next generation networks, ISO/IEC JTC1 WG7 is working on Sensor Networks, and OGC. ® SWE is working on discovery, publishing, and geo-data in an interoperable way. The main objective of GRIFS is to solve problems faced by users and organizations in a neutral way, by giving their own space. The RFID standardization process is facing lots of hurdles in the development of the relevant standards. There are a number of standards developed by various organizations, which becomes a challenge for the users for selecting the required one. These developed standards pose problems in understanding the interoperability of standards. Organizations are developing synonyms with redundancy due to lack of

communication between them. The main goal of the GRIFS standardization body is to take care of the various standards effectively in all the above cases.

2.2.1 Analysis on difference between generic concrete IoT architecture and basic IoT architecture

Basic IoT architecture has a component arrangement based on the key functions of IoT. These functions can be as follows. The main requirement is to make available object information to the user from anyplace at any time. It is connecting an object to an object or to the Internet. Here, for an Internet connection low waist TCP/IP protocol should be available with constrained objects. While completing the above requirements many other sub requirements come into the picture and can be made as generic requirements.

1. Unique object naming for each and every object.
2. Communication through any type of networks using various protocols stacks i.e. heterogeneous interoperability of data, services, and technologies.
3. Security in all types of networks, node self security.
4. Service discovery from the user/device side.
5. Provision for connecting any object at any level. I.e. device adaptability.
6. Information carrying, transferring, mining, filtering, and all data related methods for user or device query.

The above requirements are basic functionalities of IoT, and have to be converted with a generic solution. But from the concrete generic architecture point of view we need to take into account the following requirements additionally.

7. Data storage means – To handle storage of huge generated data.
8. Energy consumption for generic IoT architecture requirements.
9. Scalability – it is different than reusability. Logic should help in vertical and horizontal scalability of the network and accordingly each and every resource in it. It means scalability in all the generic requirements is expected.

IoT-A has covered all the basic generic architecture requirements (1 to 6). But the remaining three are not covered. Our research tries to focus on the development of concrete generic IoT architecture. Study further analyzes individual papers and EU projects for all the above requirements (1 to 9), and focuses that very less work is found for the last three requirements. No research is found with a specific focus on energy consumption.

2.2.2 EU and Public project's efforts

This section reveals the efforts in designing generic concrete IoT architecture. Table II states IoT features, covered challenges, and other perspective details of individual research papers

and some EU projects. Table 2-II indicates the individual IoT architecture completeness with the perspectives covered. Table IV suggests a few modifications in these architectures.

Table 2-II: Important Features from Paper and EU Projects Architecture

Paper Ref. No	Architectural metric	Building blocks	IoT features covered	Challenge	Applications
[18]	Scalability	Unit IoT module, global IoT Module	1. Ubiquitous, systematic hierarchy to connect entire world using IoT with security, safety, freedom, and restrictions at each level, 2.Standardization.	1. Designing such architecture itself is a challenge-	Industrial, Environmental, Societal.
[19]	Heterogeneous interoperability	Mobile device as a reader, wireless internet.	1. Tracking and tracing. 2. Safety.	Security.	Cooking ,washing
[20]	Heterogeneous interoperability	Wireless sensor network, cellular network, and Internet	1. RRM algorithm to provide Internet connectivity to all sensor nodes within WSN and some scattered nodes in CN covering heterogeneity. 2. RRM achieves capacity gain over the WSN and CN access and spectrum.	1. For All type of networks in IoT Such algorithm can be found out.	Telecommunication applications in selecting access technique and spectrum.
[21]	Heterogeneous interoperability	Different types of RFIDs.	1. Address mapping problem of variety of RFIDs at MAC layer is considered with a new suggested protocol. General Identity Protocol (GIP).	1. To check the computational complexity. 2. To reduce the length of header, add security, improve QOS performance.	In all IoT applications.
[22]	Device adaptability	WSN, wired or wireless Internet as per requirement.	1. Intelligence is provided with different types of contexts.	1. Achieving self capabilities.	Intelligent power grid.
[23]	Web of things, resource oriented	Web services, and smart objects.	1. Web based search for things information, enterprise services, business intelligence, and easy implementation of applications.	1. Providing web pages for all things speed of operation, service discovery.	Web based services, energy monitoring, and control systems.
[24]	Service oriented architecture	WSN, Web 2.0 Embedded web server.	1. Real world data and their functionality as part of Web. 2. REST ful approach of Web. 3. Smart gateways or embedded web servers for some devices, which cannot connect to the Internet.	1. Adapting client – server architecture. 2. Asynchronous bidirectional communication. 3. Search and discovery of smart things by browsing HTML pages is impossible.	Smart meters, energy aware web dashboard, and a physical mash up. Editor like pop fly or yahoo pipes can help in any building application.
CERP projects					
[25] Cute-Loop	Heterogeneous interoperability, security, and trust, device adaptability, service oriented, event driven architectures and more.		1. Decentralized intelligence is provided. 2. Supports features for all types of architectures mentioned. 3. Services on heterogeneous sensor, GPS or RFID readers. 4. Key elements for framework Network devices enabled services (NDEI).	1. Decoupling, heterogeneity, 2.Distribution and decentralization, 3.Connectivity, scalability, and cost and Trust.	Food chain and craftsmen business world.
[26] SMART	Service oriented architecture and many more.	RFID integrated.	Shelf inventory tracking, smart recall, promotional management, and dynamic pricing system. Case and item level tagging, innovative consumer applications, and promotion management system.	1.Redability, data management, and aggregation. 2.Consumer privacy, health corners, organisational impact, and support.	Supply chain services in retail industry.
[27] TRACER	Service oriented architecture more	RFID, client server architecture, and Web Services.	1. Any standard can be applied for identifiers and network operations.	1. Tag readability, technical and financial. 2. Cross company transparency.	Entry level solution package for very small industry or users who require lightweight tracking.

ASPIRE - [28] HYDRA- [29]	Heterogeneous interoperability and more.	Middleware, JMX management module.	1. Implements EPC standards. 2. Business events generator with filters. 3. Connector application 4. Actuators and IDE.	1. Different layers of communication architecture from different business contexts. 2. Middleware design for a reducing a high entry cost for RFID/Sensor technology adopters, and SMEs.	Logistics, textile, apparel, cold chain management, and process management.
[30] STOL PAN	Heterogeneous interoperability, SOA and more.	Mobile RFID reader, NFC, service, and distributed wireless and wired devices.	1. Implemented tracking and tracing for individual small scale company level, without connecting it to the internet.	1. Challenges are standardization in HI, business and logistic models.	Applications related with smart mobile and smart things.

Table III: Number of Features Covered in surveyed Architectures

Features / Perspectives								**CuteLoop**	**SMART**	**TRACER**	**ASPIRE Hydra**	**STOLPLAN**
Paper ref no.	**26**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28-30**	**31**
Het. Interoperability		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
Discovery mechanisms								✓				
Security and privacy						✓	✓	✓			✓	
Device adaptability					✓	✓		✓	✓	✓	✓	✓
Scalability	✓										✓	
Data volume								✓				
Energy Consumption												

Table IV: Recommendations towards Surveyed Architecture

Paper no	Comments
18	The author has taken into consideration only scalability metrics. Effect of IoT perspectives on scalability is not discussed. Other perspectives or metrics along with standardization have to be taken into consideration.
21	The author is trying to develop the address mapping techniques for different RFIDs. Provision shall be provided in advance to absorb all smart things within a standard and outside the standard with future scalability. The address scalability and security has to be considered for addressing.
22	All self capabilities shall be considered for generating contexts. Adding Intelligence will play a major role.
25 CuteLoop	1. Scalability and data volumes have to be concentrated more. 2. Discovery mechanisms from all aspects such as centralized, distributed, decentralized, syntactical , hybrid, and semantical have to be considered. 3. From centralized to decentralized shift, some control shall be kept for the central server. Centralized decisions shall be taken for decision actions in important situations. They shall be recorded properly, with filtering.
26 *SMART*	Changes in SOA and service discovery are suggested. In government owned shops, special features shall be provided for people to know details of the information available like duration, and cost along with policy. The complete information of the policies shall be made available to the customer.
27 TraSer	TraSer server can be connected to ONS and EPC for special smart things in applications with restricted entry, with much less charges as per the turnover of the individual server. This will give some motivation and guidance to improve lower end applications. Other higher class should be in a state to access the information or services of these applications, which will lead to increasing the business. Otherwise, there will not be any exchange of information and updates. There will be monopoly of some companies.
28-30 Aspire- Hydra	Filtering shall be applicable at all levels i.e. at data, security, heterogeneity of networks and devices, discovery services, customer services, and events to control the scalability of the architecture. This will indirectly reduce the execution time, improving life of infrastructure, and power consumption. Intelligence can be Introduced.
31 StolPan	There are limited numbers of predefined applications, which can be loaded. Indirect data scalability and service delivery may pose a problem. Effect on services when simultaneously Zigbee, Bluetooth, and NFC are active, can be studied.

2.2.3. Lessons learnt in various IoT projects discussed above

SToP: - Project takes into account logic for authentication. No one authentication technology is suitable for different products. Network technology, constrains on product, hardware and software platforms used can be different, leading to vulnerabilities and variation in authentication techniques. For distributed systems this logic is not applicable. But for the above type of applications, implemented authentication logic seems to be good. It has to be analyzed and selected further. There is a problem of computational capacity of individual objects. There has to be a match between wireless technology and computational capability.

BRIDGE: - IoT applications have different data features. These features have to be studied for possible anomalies and derivations in applications. It is advised that first improve the physical installations to improve reliability and eliminate spurious reads. Depending only on algorithms is not practical. Discovery systems shall take into account sensors and agents. There is a lot of scope further to develop business models for operators of discovery services, and models for serial level information between partners with low cost. Supply chain data sharing is very important in anti-counterfeiting investigations. Network based traceability is more beneficial than document centric traceability. Dynamic read point for RFID will reduce the cost considerably. There is a speed gap between machines and a human. This gap can be minimized to some extent by following decided steps, and by training operators. Significant time saving in inventory checks is possible and less staff is required. It is important to train people for commercialization of business analytics using RFID data.

CuteLoop: - Project focuses on distributed applications and covers heterogeneous interoperability. Project reveals that the researchers need to focus ubiquitous connectivity. There is a lot of scope for reducing power consumption by providing different types of RFID tags and networking devices like hubs etc. Communication means have to be finalized for low power consumption with reducing costs. The governance of diverse heterogeneous networked devices, each type including certain data fragments, features, and interfaces should be minimized to as many as possible.

STOLPAN:- Focus has to be on multi application operations. Even if a person is a registered user, too much information can be irritating. Provisions shall be made available to stop or start this communication. Various applications with different distances shall be listed. If a bigger number of applications are found for a distance more than the NFC range, then research shall be carried out to accommodate them for increasing or decreasing the range distance. Multiple services need a framework, which will support operating, technical, and business processes.

SMART: - 1. The readability of the RFID tag is influenced by the electromagnetic nature of RFID. Points, which affect this are line-of-sight, material of the tagged items and surfaces of the surrounding area, multi-path effect, tag collisions, tag positions, and environmental conditions.

a. Data management and aggregation issues of RFID reader fails to read a valid tag in a given reading cycle. This happens when a customer picks up the product to see it. A problem occurs because the product goes out of range of the readers antena range for a short time interval. Because of the absence of the product, the inventory database is updataed accordingly for the number of less products, (which is picked up).The database is again replenished, when the product is placed again.The problem is solved by using a local temporary database or buffer for such small pick ups and replacements of products at the place. This product is checked against its inventory in this buffer and accordingly, the buffer and main inventory is updataed.

b. Multiple consequent reads – creates a problem of wrong entries, i.e. the reader may read the tag when it is not expected from a location, or it may re-register a missing tag after multiple consequent reads.

Non Technical lessons

2. Consumer privacy – If disclaimer signs that are are placed on the product stand, the consumer has the privacy to read the facts of products. But this results in less sale of the products. Disclaimer signs are good for the consumer, but not for the sellers.

3. Health concerns- Because of media advertisements about the harmful radiotions of mobile and bas station, the customers ask for proof if the RFID antenas radiation is hamless to their health. But when the antenas were hidden , no questions were asked.

2.2.4. Standardization group activities

GRIFs standardization [32 activities-were missing in IoT-A survey. An overview of GRIFs is presented here, which is contributing in IoT architecture standardization. We explain GRIF as one standardization architecture (Ref fig 2.2), which explains why standardization is important and the challenges in front of it.

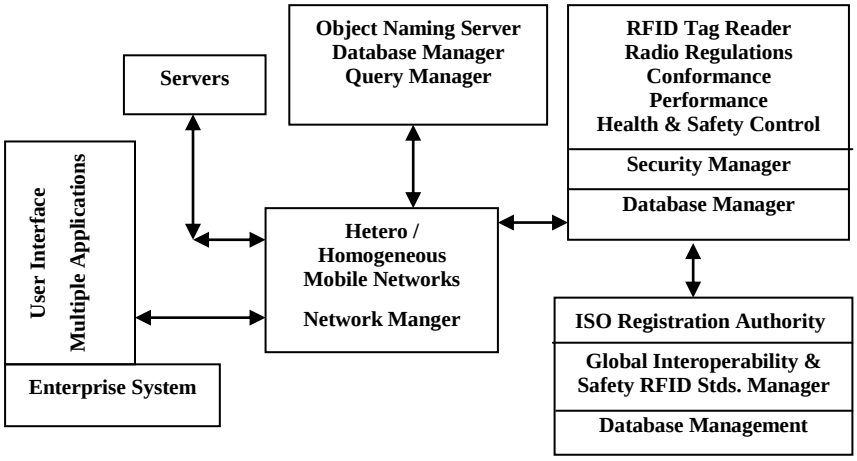


Fig 2.2: GRIFS architecture

The RFID standardization process is facing lots of hurdles in the development of the relevant standards. There are a number of standards developed by various organizations, which is a challenge for the users for selecting the required one. These developed standards pose problems in understanding the interoperability of standards. Organizations are developing synonyms with redundancy due to lack of communication between them. The objective of GRIFS is to solve problems faced by the users and organizations in a neutral way, by giving their own space.

The main goal of GRIFS architecture is to take care of different standards effectively. Architecture has blocks such as enterprise system (an enterprise instead of a single user), internal and external to enterprise data exchange components (Internetwork), and ISO Registration Authority for data formats for data conversion legacy. The major part is a component, which takes care of the above mentioned users and organizational problems with the help of the databases. Architecture takes care of real time location standards, security standards for data and networks, data exchange standards and protocols, environmental

regulations (e.g. WEEE, packaging waste), data standards, data encoding and protocol standards, device interface standards, conformance and performance standards, health and safety regulations, frequency regulations, data protection and privacy regulations, air interface standards, sensor standards of interoperability, establishment of a central and global library of regulations, which is updated regularly to satisfy the design and support needs.

2.2.5 Analysis

Firstly, we conclude that the IoT definition can be made final as "**IoT is a class/structure of fields time, place, Thing, user, object_under_focus, internet, hardware, software, and related functions for efficient, accurate, economical, direct and indirect communications to monitor or control an object in all aspects meant for communication. These fields can have all possible values or nested classes/structures. ".** It will be better to define it at an abstract level, so that it can absorb any change in future. All new means that come under above fields will be considered as a part of IoT. We can conclude that the development of concrete IoT architecture is missing because of a definition only.

Our definition shall be worthy for developing concrete generic IoT architecture. Once the architecture is complete, making changes in it will become difficult. So, all the requirements, and sub-requirements for achieving generic functions of IoT have to be dealt with. The effect of all the requirements on one another shall be studied further. All the views of architectures will help in finalizing the concrete generic architecture.

Standardization is equally important, otherwise, there will be confusion as to, follow what? While maintaining standardization metrics, scope shall be provided for other lower class development, which doesn't fit into this metrics. For example, ASPIRE and HYDRA is taking care of non standardized constrained devices. The standardization hierarchy can be produced to absorb each and every device, service, or part of IoT. This will help in developing the lower ends. For example, TraSer is giving scope to the lower class light weight applications of SMEs, or very small scale industries. When utilization is there from all the classes and levels, in the true sense IoT will come into the picture.

2.3. State of the Art on Communication Protocols

2.3.1. Papers contribution

There is a huge heterogeneity of network technologies, devices, infrastructures, and data types (static or dynamic) available. There is a requirement of a unique IoT communication protocol, which will handle the above heterogeneity. Various protocols satisfying the IoT communication requirements are going to be a combination of various communication stages (indirectly, the implementation of protocols one after the other at different places and as per Requirement) from Thing to an internet or the Internet. These various protocols for a series of intermediate various scenarios need to be identified and standardized. IoT is an extension of the Internet with various options for access of devices with technology e.g. GPRS/CDMA, short message, sensor, and cable. Paper [33] has done this job and found out such various stages and their protocols as UID registration, UID cancellation, UID search, information, inquiry, and step-over UID information protocol.

Wireless IoT communication stacks the major requirements, which are power efficiency, reliability, and Internet connectivity. Paper [34] written by senior IEEE members proposes the protocols stack by using key embodiments of low power efficient IEEE 802.15.4-2006 PHY layer. The power saving and reliable IEEE 802.15.4e MAC layer, the IETF 6LoWPAN [35] adaptation layer enabling universal connectivity, the IETF ROLL routing protocol (Network layer) for availability and IETF CoAP for seamless (transport and application layer) transport, and support of Internet applications. Paper has proposed stack with the detailed survey of the development path of the above standards for the mentioned layers.

Protocols operating at multiple layers for embedded and communication objects, and protocols operating at a single layer are available in [36], along with standardization.

2.3.2. Protocols Operating Across Multiple Layers

Multiple layer means, multiple interfaces (physical layers) and multiple links for communication. In multi-homing, various combinations are possible like Single Link-Multiple IP address, Multiple Interfaces- Single IP address per interface, Multiple Links-Single IP address, and Multiple Links- Multiple IP address. For multiple links, when one of the links fails, the protocol notices this on both sides and traffic is not sent over the failing link any more. This method is usually employed to multi-home a site and not for single hosts. For multiple interfaces, the host has multiple network interface controllers (NICs) and each interface has one, or more, IP addresses. Either link can break the IP address. When the link fails, the IP address can be used on another interface, with timeout penalty. Such situations

can be handled by Stream Control Transmission Protocol (SCTP) [37], and Host Identity Protocol (HIP) [38]. SCTP helps in taking the existing connection over the other interface, which is not possible in TCP.SCTP is an alternative for TCP and UDP. It has multi-streaming and multi-homing , mobility support without special routing support, error free and non-duplicated data transfer, resistance to flooding, and network level fault tolerance are some of the features of SCTP.

2.3.3. Protocols Operating Across Single Layer

Protocols that are implemented for establishing a direct connection between two networking nodes come under this category. I.e. data link protocols e.g. (PPP) protocol commonly used in establishing a connection (single or multiple networks). It can provide connection authentication, transmission encryption , and compression. PPP is used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fibre optic links such as SONET.

Communication enabled devices use different physical layer interfaces as per application requirements. There are some devices, which are connected to the internet through some platform such as gateways, mobile phones, or application specific IP-enabled points of access (e.g. object readers). Most of these devices (small size, lightweight, low cost) implement protocols up to a network layer. 802.15. x. PAN objects implement protocols up to link layers only. It is observed that most of the higher level protocols of communication objects are tailored as per the network requirements and they do not apply IP based TCP-UDP protocols. Serial, USB, CAN, and Profi bus implements protocols up to link layers only, and they connect directly to the microcontrollers of these devices.

802.15. X Series (Zigbee, Bluetooth, RFID, etc.), Wi-Fi, and UWB wireless communications implements NWK/APS/API, IP/TCP-UDP, and Baseband/Link Manager/L2CAP (non-IP) protocols respectively. Serial, USB (wireless), Sensor network busses (e.g. CAN [39], Profibus [40], etc.), DeviceNet and ControlNet [41], Power line (KNX, LonWorks) protocols [42-43] are of fixed communication type. The first three implement protocols up to the data link layer. DeviceNet and ControlNet require their own customized protocols for an individual network. Power line networks implement Network/transport layers according to KNX and LonWorks specifications.

There is some category of devices that has compatibility towards IP, TCP, UDP protocols or inbuilt IP, TCP, and UDP protocols for connectivity towards public internet. KNX and LonWorks standards refer to the first type and Ethernet/IP technology. Wi-Fi comes under the second type.

2.3.4. IP networking technologies

This section is made up of two parts. The first part explains the various protocols for connecting an object (or group of objects) to the Internet continuously when they are moving. The second part explains the various protocols, which are required for connecting these objects to the web and Internet.

2.3.4.1. As it is a requirement of all communication objects to be connected to the Internet, the efforts led to solutions for embedded TCP/IP stacks like Tiny TCP, lwIP, µIP. Solutions also add to the mobility support. Mobile IP allows the devices to move, and get attached to the Internet without changing its IP address. Network mobility (NEMO) allows the complete network facility of getting connected to the Internet, without changing the device's IP addresses. SHIM6 allows the continuing one node communication with the other node, even if, any one node loses its IP address. It can be called as server- less mobile IPv6 protocol. This is possible when two nodes have applied number of protocols (for various situations of scenarios') for the generation of contexts of the locators, for finding each other. SCTP, HIP, MIP [44], and SHIM6 [45] all support identifier –locator split supports. SCTP signifies shared secret or address configuration, HIP implements new locator information within IPsec ESP tunnel, MIP specifies return routability procedures, and SHIM6 features locator update as the identifier for locator binding.

2.3.4.2. Different network architecture will be there for constrained (energy limited) and non-constrained (no energy limitation) nodes. Section explains architecture for constrained node and core node and is n in figure 2.3. Various communication scenarios will be present. Nodes in the IoT have very limited computing power and according to this, the payload overheads have to be removed. SOAP based and RESTful Web based services are available. But the RESTful approach is implemented, as it is lightweight. The overall requirement of a protocol is lightweight.

SoAP – It is the simple object access protocol meant for the web server and IP enabled computer communication network. Web services apply HTTP for message communication. SoAP is based on XML and has three parts as an envelope for message contents and processing on them, encoding rules for instances of application data types, and rules for representation of procedure calls and responses. The drawback of the XML based formats are their size. The XML format is verbose and therefore, is not suitable for low power and low data rate sensor networks leading to the unpopularity of SoAP.

CoAP [46] – Device shall be able to create, read, update, and delete resource information on its own. Changes of device or things resources information is communicated to the other

device using CoAP protocol. Constrained application protocol is specifically designed for web transfer, with constrained nodes (8 bit micro- controllers) and networks (6LoWPAN, low- power lossy network). It is an application layer protocol for constrained embedded devices (M2M). It has built in discovery of services and recourses. It supports e Uniform Resource Identifiers (URIs) and Internet media types as key concepts of the web. It can easily interface with HTTP for integration in web with multicasting, very low overhead, and simplicity for constrained networks. EXI is a compressed XML language for simple and uniform description of data. For constrained (7 kB ROM and 1 kB of RAM) devices it is suitable along with CoAP protocol.

6LoWPAN [47] - is an acronym for IPv6 over low power wireless personal area networks. Encapsulation and compression mechanisms on IPv6 makes, the IP protocol suitable for constrained devices and known as 6LoWPAN.

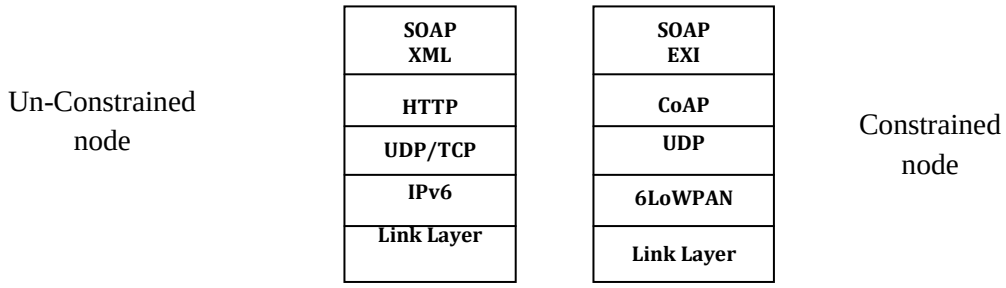


Figure 2.3: Unconstrained (core) and constrained node protocol stack

µ IP (micro IP) and lwIP (lightweight IP) [48] - are implementations of generic and portable TCP/IP, which has enabled the vision of IoT come true. LwIP is TCP/IP's full scale simplified version, includes IP, ICMP, UDP, and TCP and has modular features. Multiple local interfaces and a flexible configuration feature make it suitable for many devices. **µ**IP has absolute minimum features of TCP/IP stack. It handles single interface, IP, ICMP, and TCP protocols. It does not support UDP. Implementation on 8 and 16 bit platforms is a special feature of both protocols. These two stacks allow to network client and server of 8 bits, very low RAM and ROM size and low power, which is not the case with the other existing TCP/IP implementations. µIP has made it possible to connect constrained devices to the Internet. Table V states all the features in both protocols. There are lots of requirements of TCP/IP protocol stack. Most of the features are implemented in **µ**IP except a few, such as soft error reporting mechanism and dynamically configurable type-of-service bits for TCP connections are not implemented as very few applications make use of them.

TABLE V: TCP/IP Features Implemented In µIP and LwIP [48]

Feature	µ IP	lwIP
IP and TCP checksums, IP fragment reassembly.	Y	Y
IP options	N	N
Multiple interfaces	N	Y
UDP	N	Y
Multiple TCP connections, TCP options, and TCP urgent data	Y	Y
RTT estimation, Variable TCP MSS, and TCP flow control	Y	Y
Sliding TCP window	__	Y
TCP congestion control	Not needed	Y
Out-of-sequence TCP data	__	Y
Data buffered for re-xmit	__	Y

2.3.5 Protocols under Standardization Workgroups

Standardization activity has three working groups for the IoT protocol. They are Routing over Low power and lossy networks (ROLL), IPv6 for low power PAN (6LoWPAN), and constrained RESTful environments (CORE).

2.3.5.1. ROLL [49]

RoLL has *resource-constrained* devices, using IEEE 802.15.4, Bluetooth, Low power Wi-Fi, Wired or Low power PLC (power line communication). Communication links have problems such as high loss rates, low data rate, and variable instability. At present, several routing protocols for distributed ad hoc networks are available. But ROLL WG has started developing the application based routing protocol for low power and Lossy networks (RIL). IPv6 based architecture and security and self configuration are some of the important features, which are targeted. The following subsections discuss various protocols, as per the application scenario.

2.3.5.2. URBAN LOW-POWER AND LOSSY NETWORKS (U-LLn)

Sensors, actuators, and routers implement wireless communication based on IEEE 802.15.4, Low power IEEE 802.11, or IEEE 802.15.1 (Bluetooth). Industrial routing low power and lossy network (LLN) [50] has field devices placed in various plant environments and in turn has different routing, security, throughput, and delay requirements. Focus is on safety, control, and monitoring. Emergency action environment (always critical) situations are considered for safety. Critical functions in closed loop regulatory control, non-critical functions in open loop supervisory control, and operator takes action and controls the actuators in open loop are considered for control. Short term operational effects in alerting situations, logging and downloading / uploading situations for monitoring are focused. Future houses [51] will have provisions for monitoring, controlling of actuators, or advanced servers

as automation requirements. These devices have limited resources, requiring multi-hop routing. ROLL recommends on how building management systems (BMSs) [52] should be built. BMS is a hierarchical system of sensors, actuators, controllers, and user interfaces and should interoperate to provide a safe and comfortable environment. ROLL has another protocol as RPL based on IPv6 routing and trickle algorithm.

2.3.5.3. 6LowPAN WG

LoWPANs are characterized by encapsulation and header compression that allows IPv6 packets to be communicated on the 802.15.4 physical layer. IETF workgroup 6LoWPAN has introduced an adaptation layer to overcome large IP address and headers, minimum transfer unit (fragmentation), to allow sending and receiving packets over IEEE802.15.4 networks. This adaptation layer has been introduced as a MAC layer.

2.3.5.4. Constrained RESTful (CoRE) WG

Provides the framework for limited applications where simple monitoring is required. A framework for resource oriented applications running on constrained IP based devices. WG aims for RESTful Web based protocol for most constrained embedded devices and networks. CoAP supports datagram transports such as UDP or DTLS limiting the maximum size of resource representation without too much fragmentation. Instead of using IP fragmentation, CoAP supports multiple block transfers from resource representation in a request response manner. Protocol client observes the CoAP server over a period of time. It has a stateless server and client leading to a small cache. It supports semantic contents for the exchange of messages.

2.3.5.5. Lightweight IP Protocol Stacks IETF WG

Work group Implements the TCP/IP protocol on constrained devices. There is no proper documentation available for its implementation. It is working on Documents formation for problem statement and common issues by the implementers, implementation techniques, mentioning challenges, and realization in relation with memory and energy optimization. It has created the profiles for lightweight, minimal IP implementations and provides a guideline for IP implementations with minimal functionalities required for interoperability with the existing TCP/IP stacks.

2.4. Network Architecture State of the Art

IoT is a combination [53] of core network and peripheral networks. Core network nodes have sufficient required computing power which may not be the case with peripheral nodes. Peripheral networks are divided further as constrained and unconstrained nodes. Computing power will decide the network stack that can be implemented by the individual nodes. Core

network will apply standard TCP/IP stack, but for low power devices like 802.15.4, stack has compressed payload and TCP frames. Again data is transmitted in the fragmented form and has to be reconstructed at the receiver side. This adaptation as per nodes computing power will vary.

2.4.1. Core and Peripheral network stacks

Core network stack is presented in figure 2-4. Some changes required at the stacks are also mentioned below. Considering future requirements network management layer shall be added as an extra layer.

Peripheral Network – various networking technologies exist for different wireless ranges like Bluetooth, Zigbee, Wi-Fi, UMT etc. nodes which has low computing power cannot implement the same stack as the, core network. Node can be moving or static. There are many communication scenarios like uni-cast and multicast together, uni-cast, multicast, or any-cast for constrained devices. Paper [116] has presented general stack for the constrained devices. Accordingly small changes in the services will vary. IPV4 to IPV6 is tackled in paper [54]. Paper puts further that this mapping is sufficient from the network layer point of view, but mapping of network layer address to data link layer address is not resolved. Many applications propose IoT architecture required for its own execution. The stack which can be upgraded is as presented in figure 3.8. Services required from IoT point of view are only mentioned, at the different layers are as follows. It is assumed that basic requirements of all layers, other than mentioned are present.

1. Physical layer – It should be able to sense all types of devices. Device adaptability is the main requirement of this layer along with its standard services.
2. MAC layer – different type of interfaces shall be used here.
3. Adaptation layer – The main task is to adapt the stack as per the computing power and convert the payload and headers as per the requirement. Compression of TCP/IP header as per requirement should be followed. The layer should support the feature of virtualization from increasing the scalability of the network.
4. Network layer – If things are stationary, responsibility is to only find the correct addressed node. If things are moving they should be able to handle the horizontal and vertical handoffs. Also instead of IPV4 addressing, IPV6 addressing shall be applied. The layer should be able to find the physical address and then virtual address, for scalability.
5. Transport layer – transporting the packets to the destination shall continue as it is. In peripheral network TCP/IP protocol can be with compressed headers.

6. Presentation layer – For IoT it is expected that, data will be sent from Things to server. Considering the case, no presentation is required as such all information will be sent in the form of messages. Simple data formats are expected like XML data formats. QoS requirements shall be decided here only.

2.4.2. Analysis - IP networking technologies for mobile constrained nodes face lots of QoS problems and they vary as per the number of nodes in the network. QoS parameters like Bandwidth, time for handover, and throughput in a dynamic scalable wireless network are difficult to attain a required standard.

While designing protocols the following all points of the network should be taken into account. As per the constraints of a node compression, decompression, and fragmentation of packets shall be done in the stack. UDP offers compression and fragmentation in 6LoWPAN, and TCP does not offer fragmentation. UDP fragmentation is supported up to 64 KiB. Larger payloads don't really work well for constrained applications and networks. Block transfers are promoted in CoAP. CoAP publishes resource data and authorizes for a subscribed node only. When data is transferred to many nodes, the reliability of data transfer shall be achieved. At present it is not there for multicast or any cast communication. Security and privacy comes into the picture when the resource information is published. Stateless client and server CoAP may lead to loss of data. SoAP based web protocols use XML language.

EXI and JSON are some of the better messaging languages than XML. Various OS should have library support for better results of CoAP. For IoT, uni-cast, multicast, reverse multicast, any-cast, and broadcast type of communications can be there. There can be various scenarios of communication, between various types of communications as mentioned above. Delay tolerant networking can be implemented with the Internet and sensor network to cope up with long delays and un-predictable delays. The node should run the TCP/IP protocol suite, which can eliminate the use of proxy and gateways. The possible combination of DTN overlay, TCP/IP, and proxy or an individual solution shall be adopted.

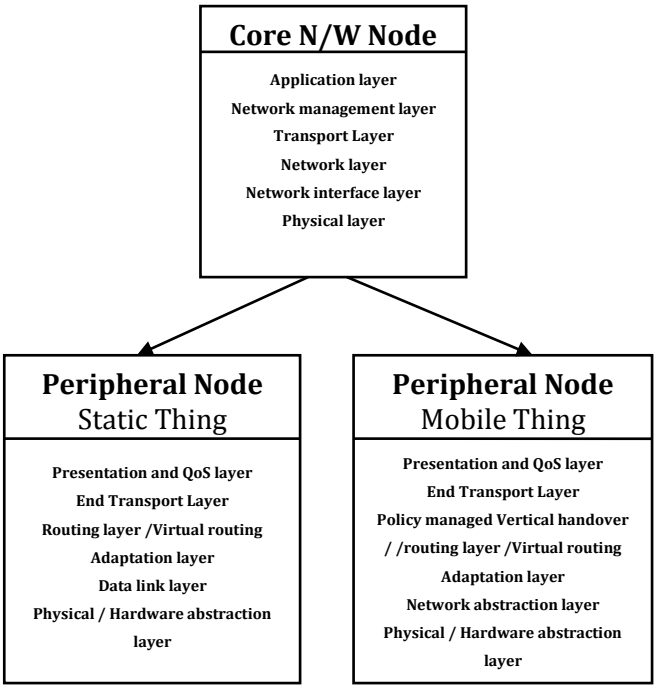


Fig 2-4: Core and Peripheral Networks layers for IoT

A comprehensive solution, which will allow different levels of communication stack to interact with one another and with different technologies, has to be worked further. For IP compatibility 6LoWPAN, CORE, and COAP the existing standards can be applied. Considering all the scenarios of communication, three major communication stacks are required as constrained, unconstrained, and below constrained. In below constrained category simple data transfer and reception shall takes place without any addressing, routing procedures, or security means.

2.5. State of the Art of Security

IoT is ubiquitous and pervasive in nature and so is security. Accordingly, a great amount of data will be available from its ubiquitous networks. Ubiquitous and pervasive networks will create security problems. These problems may be because of data generated, physical attacks, privacy of data, and attacks due to the wireless medium. Physical attacks are difficult to deal with in relation with the tiny node of IoT. A secure system has three main functions as authenticity, confidentiality, and integrity. Privacy has measures like transparency, verifiability, and integrity in relation with personal information.

2.5.1 SECURITY

It can be analyzed as legacy internet attacks and peripheral IoT devices attacks, due to their vulnerabilities. Legacy Internet attacks security framework (is provided in chapter five) and their solutions are already available. As IoT is new technology, where all attacks are not known. We focus our attention to new security attacks. IoT physical devices can be RFID,

NFC, and wireless sensor and actuator devices. Each has different vulnerabilities along with the wireless link as the biggest problem. All attacks in table VI are carried on a physical layer. Device wise attacks and their state of the art are listed below.

TABLE VI: State of the Art of Attacks on RFID

Eavesdropping Attack	Technique used	Research required to be done
Eavesdrop	Listens, captures messages because of weakness of contact links	Methodology used to handle attacks along with tests and results are required. Research done [55-57] is not giving sufficient information on tests and results. The encryption method of data with fewer bits is required. E.G. Skimming Distance for capturing varies from 2103.12 cm to 35cm [56].
Denial of Service	Protective means help attackers, emit a signal in the same bandwidth of reader to blur the data.	Blocker tag [57], RFID guardian, Reader and jamming attack are not detailed.
Man in the middle [58]	Retrieves cryptographic keys	Time out period of reader has to be improved.
Side channel	Carrier Radio frequency analysis for retrieving cryptographic keys	No solution is available yet for IoT.
Hardware [59] destruction	Chemical, mechanical, magnetic field, microwave oven use, zener diodes, self healing fuses.	No absolute protection against electromagnetic field.
Software [59] destruction	Use of commands, keys, passwords or other methods	Not much Research is available for IoT.
Counterfeiting, replay attacks, substitution.	Reprogramming of microprocessor or RFID tag, tampering a chip for unique information.	No solution is available yet for IoT.

Near field communications (NFC) - systems have the same vulnerabilities as RFID systems. Additional attacks are due to their use cases, inner architectures, and their technical capabilities. User tracking, relay attack, and eavesdropping are some of common attacks as RFID. Malicious host applications [59] allow the attacker to gain control of the application processor. Some use cases that are vulnerable to fishing attack [59]. Viral attack [59] is spread due to bidirectional communication.

TABLE VII: State of the Art of Attacks on WSAN

Layer	Attack name	Technique used	Research to be done
Transport	Ping/ICMP flood , smurf [60] attack	Consumes bandwidth with different types of packets like ICMP, UDP, TCPXMAS flood, IP of target for flooding the bandwidth and time of CPU.	These attacks are absolute on the internet, but need to be considered on WSAN and IoT.
	Synflood [60-61]	Creates a false impression that the socket is open at both ends.	Cookies, Syn cache, and exploitation of timestamp field of SYN message are some of the solutions. But they require more memory, which is a constraint in WASN and IoT.
Network	Neighbors discovery	Attacks make believe the target node that they provide network functionalities to alter the topology and disrupt the traffic.	ND protocol does not provide any security features. For WSAN and IoT better solutions shall be found out. Redirect attack [62-63] cannot depend on the NDP trust model.
	Wormhole [64]	Transmission of packet to the out of range target.	**Research** is required on dynamic WSAN.
	Black / grey hole , co-operative [65]	Distance vector based protocols are more vulnerable.	Scope of improvement in available solutions for co-operative grey hole attacks.
Link layer	Collision, exhaustive, denial-of-sleep	Uses the WPAN channel to occupy bandwidth and depletes battery supply.	Better solution for wireless embedded devices is required as available solutions affect bandwidth and, which is a constraint for IoT devices.

Wireless sensor and actuators – Constraint of battery life becomes the biggest vulnerability for security attacks. Jamming, tampering, and eavesdropping attacks are the same as RFID. Other attacks are listed in table VII.

2.5.2. Analysis - Smaller encryption key is expected. Smaller key sizes can be achieved with public key based solutions with energy efficiency, secure communications, and less storage. Scalability of security architectures is expected.

The biggest threat is from the physical layer. Here, physical authentication is not secured and results in forging and replaying of packets. It is difficult to make a secure wireless IoT communication due to the constrained bandwidth, processing power, and power resources. Gateways or RFID readers should provide mechanisms for security. Gateways should support authentication and access management. In the ubiquitous and pervasive IoT, security will continue to be a major research area in future.

2.6. State of the Art in Identification and Resolution Frameworks

2.6.1. Identification Contributions

Table VIII summarizes the review of identification, naming and addressing schemes, and frameworks for IoT. Naming refers to giving a name, addressing refers to placing the object in space, and look-up refers to finding a suitable object, then resolving its name to get an address.

TABLE VIII: Identification Methods from Various Projects

Project name	Identification methods
SENSEI	Resource ID is formed by concatenating the domain of resource's provider, and the type of device, a name representative of the resource's function, and a unique identifier.
uID Framework [66]	Identification is done by 128 bit ucode and is retrieved from the database servers.
EPC global [67]	Identification is based on the URI model.
DIALOG [68]	Uses ID@URI.It uses some properties of EPC/ONS, and it also supports barcodes.
Host Identity Protocol (HIP)	The identity should remain the same even if the location changes and this can be implemented by locator-identifier's split logic.
Connected Objects (CO)	Uses host identity based on public and private keys, and identification can be unique or overlapping.
International Mobile Equipment Identity (IMEI) [69]	Uses a set of digits that represent the manufacturer, the unit itself, and the software installed on it.

2.6.2. Addressing Styles of IoT Objects

MAC address, IP address, E-mail address, uniform resource name (URN), Uniform resource identifier (URI), uniform resource locator (URL), peer to peer addressing using hash table are some of the addressing styles indicated by ISO Stack. Resolution is a three-step function as discovery, lookup, and monitoring. Table IX abstracts an overview of the various frameworks for resolution.

TABLE IX: Resolution Frameworks

Framework	Resolution
EPC global	Framework has lookup service that stores references to EPCIS, linked to EPC numbers for the requested object.
BRIDGE	Provides directory services with the help of single or many federated servers that provide lookup for EPCIS.
	Middleware architectures Gateway can be one of the solutions for data exchange between sensor nodes and Web applications. Device Profile for Web Services (DPWS) provides WSN functionalities on the internet and provides plug and play facility. A gateway has Service directory, which stores functionalities of sensor nodes.
SOA	Requires semantic descriptions along with (DPWS) mentioned above.
SENSI	Resource providers use unique resource identifiers within their administrative domain. Resource directories concatenate the resource identifier with the domain name they belong to.

2.6.3. Commercial Contributions

SENSI and BRIDGE are some of the public contributed solutions for naming, addressing, and service discovery. QR products and Digital object identifiers are some of the commercial contributions.

2.6.4. STANDARDIZATION CONTRIBUTIONS

According to applications, the standardization bodies have fixed up some methods. EPCglobal1 relates to RFIDs and is recommended always for IoT. UID Centre allows identification for objects, places, contents, and concepts.

Car to Car Communication Consortium (C2C-CC) [70] provides vehicle identifiers using the locator –identifier split. ISO TC204 WG16 [71] provides standards for CALM (Continuous communications Air interface for Long and Medium range). WAVE is another standard for vehicular communication. The resources management part is IEEE1609.1, the WAVE security architecture and services are defined in IEEE1609.2, IEEE1609.3 defines WAVE networking services and WAVE multi-channel operations are provided by IEEE1609.4. Multiple applications registration to a roadside resource manager and its use to access onboard equipment are provided by IEEE1609.1.

Pharmaceutical identification has parallel norms in various countries, which can lead to counterfeiting and serious problems for the patients. EFPIA based on the 2D data matrix ECC-200 was rejected because of security and privacy. It is required that IoT will develop some solution for the existing problems.

Public switched telephone network (PSTN) implements E.163 [72]/E.164 (telephone no's), GSM, WCDMA, and iDEN mobile phones uses International Mobile Equipment Identity (IMEI) conforming to the 3GPP TS 22.016 5, circuit switched networks adopts some network functions as signalling Point Codes (SPC) to address networks, and packet switched

networks like the Internet and other IP based networks, the identifiers are names signified in the form of Domain Names.

2.6.5. Analysis – The above standardization study specify that a number of identification and addressing schemes are available for a logical group of objects e.g. for Pharmaceutical, vehicles etc. But at the same time we can say that interchanging identification schemes in other groups is not useful and possible. One cannot adopt Pharmaceutical identifiers for vehicles or vice versa. It can be very difficult to provide only one identification and addressing style, along with legacy practices. A solution can be to integrate all these identifiers into one single framework. A unique identifier for this integrated framework will not be appropriate, as the framework will keep on increasing as new group schemes are added. Frameworks should support for future development.

Another issue is maintaining object identity when they are moving, as their location identity changes accordingly. Object identity and location identity are two different things. So, we can think whether to take location identity as a major identity or a temporary one along with object identity. Lots of possibilities can be experimented for solving the problem. One of the important considerations shall be to include privacy and identity management in this framework.

2.7 State of the Art on IoT Object Platforms

2.7.1. Technologies

Zigbee and Bluetooth are two technologies enabling physical interfaces for low power devices. Bluetooth low energy is another technology implemented for the same. This technology is 15 times more efficient than Bluetooth. Connecting and discovering various nodes methods, and size of data packets help in improving efficiency. Ultra-wide bandwidth (UWB) [73] or impulse radio-UWB is another technology used. Ultra-wide bandwidth allows for high precision ranging communication capabilities. UWB offers a chirp spread spectrum. Z-Wave [74] developed by a Danish company focuses on remote control applications. Technology supports mesh topology with a maximum of 232 nodes, with 9.6 Kbps and 40Kbps. The range of 100m and radio standard is closed (only available to customers). RFID/NFC technologies can be differentiated based on their range of sensing and the application induced in it. Numbers of standards are available with various frequencies like 135 kHz, 13.56 MHz, 433 MHz, 860 to 950 MHz, 2.45 GHz, and 5.8 GHz for ISO 18000 standard. ISO 18000-6, ISO18000-3, ISO 15693 are a few more standards.

2.7.2. Hardware

CC2420 Radio Chip, CC2420 Radio Chip, CC2530 System on Chip Radio, MSP430 F54xx (Texas Instruments) Micro controller, Atmel Radios – AT86RF2xx, Atmel Micro Controllers, Zigbee Physical (PHY) interface, Bluetooth physical interface, Bluetooth Low Energy (LE) Technology, Ultra-Wide Bandwidth (UWB) Technology, and Z-Wave are some of the hardware and software available for IoT development. The hardware features are put up in table X. For details one can refer to the datasheets on Google.

TABLE X: Hardware Information

Component name	Features	Applications
CC2420 Radio Chip [75]	IEEE 802.15.4 complaint for unlicensed 2.4GHz ISM band, Direct sequence spread spectrum, CSMA channel access, data rate 250 kbps, low cost, programmable output power, 128 B TX, RX buffer, digital radio strength indicator, link quality indicator, battery monitor, h/w AES encryption.	Building/home automation.
CC2430 System on Chip Radio [76]	IEEE 802.15.4 compliant, low energy consumption of 0.5mA in power down and 0.3 mA in stand-by mode, fast transitions from power down to active mode with low power consumption, core with 8051 uC with 32,64,128 ISP flash, 8KB of RAM, three timers, DMA functionality, 12 bit ADC, AES security processor, and RSSI and LQI support, CSMA/CA.	Home/building automation Industrial Control and Monitoring.
CC2530 System on Chip Radio [77]	IEEE 802.15.4 compliant, variable output power, five channel DMA. Other features are the same as CC2430 with an additional flash of 256 KB,	RF remote controls. 2.4 GHz IEEE 802.15.4 systems. Home and building automation, Industrial control and monitoring, Set-top boxes Consumer electronics and smart Energy.
Micro-controllers		
MSP430 F54xx Texas Inst. [78]	Ultra low power 16 bit RISC CPU, five power modes optimized to achieve extended battery life, digital oscillators, 16bit timers,4 serial interfaces, 12 bit ADC, H/w multiplier, 87 I/O pins, alarm capabilities, flash-48KB, RAM-10KB, Clock-1MHz.	Commercial and experimental (scientific research market) products e.g. Crossbow TelosB sensor nodes, boards from Sensinode.
Atmel Microcontrollers AT mega the AT mega series. [79-80]	AT mega – ROM -4 to 256 kB ATXmega –more suitable for future WSN applications -ROM - 16-384 kB, extended features as DMA and cryptography. Reduced energy consumption, operate from 1.6to 3.6V, 32MIPS, pico-power technology achieves consumption as 1mA, 12 bit ADC.	Manufacturing industry, home automation, and auto-motive.

2.7.3. Operating Systems

In general an operating system manages resources efficiently for a wide range of applications with flexibility. In case of IoT, operating systems are characterized by resource constraints, high dynamics, and potentially inaccessible deployment. Challenges for designing the OS for IoT are at node level, network level, and at the tools level. At node level, the critical part is very limited resources like power. For better consumption, OS has to apply the sleep modes, design of API without the mixing of hardware and software codes. Event driven run to completion models are required. An OS should be able to handle the heterogeneity of the devices in a network, and it should be reconfigurable and customizable. Using the same OS on different devices nodes will solve the problem of portability.

At the network level, the main issue is whether to treat WSN as a single entity or as a distributed nature. Bandwidth variation, and link failures, shall be hidden to the application developer. Currently, there is not a single protocol, which will serve for a majority of application domains. The performance of WSN degrades in acceptable ways as the number of nodes in the network increases. It is expected that an OS should focus on base mechanisms and abstractions, building more specific high-level network protocols. Tool support is very crucial in WSN. It is expected that research is required to be done in advance before the actual application is deployed. Development of a code is recommended using oops oriented languages or C#. Test setups are complex.

TinyOS [81] and Contiki [82] are adopted explicitly for WSNs and FreeRTOS [83] is a general operating system for embedded systems. All OS are open source operating systems.

Contiki–has features like where resources are constrained very much. It is highly memory efficient and uses memory block allocation, managed memory allocator, and standard C memory allocator malloc. It selects UDP, TCP, and HTTP with low power standards like 6LowPAN, RPL, and CoAP. It operates in extremely low power systems. It picks up sleepy routers, which sleep between message relaying. To use memory economically it follows different techniques as

1) *Proto thread* – combination of event driven and multi threaded programming mechanisms.

2) *Dynamic module loading* – dynamically loads and links modules at runtime, and also optionally files can be stripped off to reduce size.

An alternative simple stack is available when bandwidth problems are there. It is known as Rime. It supports sending messages to all neighbours with, network flooding and addresses free multi-hop semi reliable scalable data collection in worst situations. A typical system with IP networking with sleepy routers and RPL routing needs less than 10k RAM and 30 K ROM.

2.7.4. Analysis – There are lot of improvements in hardware that are required. Embedded security, more range, smaller in size, and easy input output facilities are some of the required features in hardware. Low power listening throughputs and interfaces have synchronous and asynchronous methods for improvement. Naming conventions adopted for components on interfaces, packages and different languages should also be standardized, else mismatching will cause in failure. Timer is the heart of any hardware system (or micro-controller), and its abstraction and interfaces shall be very accurate. Resource sharing is dependent on virtualization and status of events completion. Abstractions available for resources shall be

able to virtualize else they cannot be implemented by multiple components. Abstractions of physical resources are important and can help in decision of virtualized, shared, or dedicated selection of resource (hardware). In all the above types of engagements, the resource arbiters decide the way in which, resource utilization is to be done. IoT OS should be event based, and single threaded with dynamic updation.

2.8. State of the Art of IoT Modelling Techniques

Modeling is a standard way to visualize the design of a system, using various activities, software components, how entities interact with each other, what are external user interfaces and how the system is expected to be used. An IoT system modeling is required to be done in static and dynamic way. In static modeling object do not change state, where as it changes the state as per events, conditions at a specific time or for duration.

Under this umbrella, we cover the modeling techniques and features useful for IoT [84]. IoT is highly dynamic and massively scalable with a resource-constrained event driven device system. Traditional tools are not able to model IoT processes based on Enterprise service and process modeling. BPM has two levels of modeling as business process and technical process. The technical level implements the technical details with the help of a process engine. IoT modeling needs to monitor stationary, dynamic objects or things, which represent the physical world. Here, asynchronous events are important. IoT events can have different approaches like complex event processing, stateful eventing, and Web events. Complex Events are classified further according to their importance or priority level like Information, Notice, Warning, Error, Alert, and so on. BPMS 2.0 can be thought of a better model for process modeling domain and service modeling domain with Universal Service Description Language (USDL). Refer table XI for modeling projects and table XII for various tools. Lots of efforts are taken for modeling sensor, networks, and resources. But still a complete solution or modeling language is not available or standardized yet.

2.8.1. IoT Modelling - research papers

Sensor models and their relationship are studied [85] technically, putting forward gaps of the existing sensor description methods. It also explores the details of sensor types, sensor services, and data types in the standardized modeling technique. Sensor description methodology like SWE and sensorML, device description language, and device Kit are explained further. Pros and cons of the existing sensor description standards with a detailed technical analysis are the unique features of paper [85]. Paper [86] provides a component based model and Insense language for sensor applications. Worst space, time usage, and

resource constrained device's features are some of the parameters considered for modeling. Modeling features have to be developed as per focus of the application.

Paper [87] describes and analyzes security models by UML for the network and transport layer. The author claims that modeling helps to analyze attacks and simplifies the design of WSNs. Data for modeling can be in any format e.g., audio, video, images, and simple data. As per data type, the modeling technique will vary. Paper [88] presents the image processing, which allows the automatic description of a sensor cell HDL format. Paper has modeled IoT as a context awareness, dynamic communication, and interaction among all objects by using their properties as a generic profile. The same logic is extended further for disaster management application. For analyzing the system, graph theory is applied. It demonstrates the application of embedded intelligence in objects to assist smart resource pairing, discovery, and the harvesting process.

There are lots of errors, noise, and drop of readings in the collected data from sensors. As sensor measurements itself are prone to various errors, it is very much essential to do error modeling. It helps in understanding and characterizing the different types of noises present in the measurement. The same fact is presented in paper [89]. Paper [90] states the crop growth IoT model along with practical experience.

2.8. 2. IoT Modelling Public Contribution

TABLE XII: Public Contribution in IoT Modelling

Project Name	Features
SemProM [91]	Provides abstractions to IoT devices like RFIDs, orchestration and administration of IoT resources using "Real World Integration Platform." Site Manager allows configuring any smart environment with simple drag and drop of respective agent instances, relation between them, and remote control of these nodes and agents running inside them is possible. Still lacks the modelling of highly dynamic environments. Static modelling is appropriate for IoT.
SENSI [92]	WS&ANs can be modelled as resources in different ways. A resource model clearly models various aspects like functionalities and accessibility of the resources. This information is found in the form of resource description in the form of resource directory. Semantic aspects are part of advanced resource description. Actuation cab is done on both resource level and context level. Scheduling of actuation tasks and conditional execution is supported.
ALLOW [93]	Basic concept is Adaptable Pervasive Flows (APF) in pervasive environments. As per changes in environment and contexts of moving entity, the flow changes can be found in environment and entity itself. Security annotations can be used to define constraints on the execution flows. All these features are allowed in BPEL designs.
LMPL Lightweight process modelling [94]	Provides forum for the community of experts of various styles of modelling. Context awareness, usability, and reusability using BPMN symbols for control flow and flexibility, and invocation of web services. Allows describing and defining IoT devices and architectures. Communication between different components can be abstracted.
SAP Gravity [95]	It allows BPM in real time. New and existing business processes can be modelled across organizational limits by various users. Various processes are n in different colours. It transforms the graphical process into executables. An individual process can be monitored by a process engine. A model can be exported into BPMN .

2.8.3. Various tools for IoT modelling

TABLE XI: Modelling Tools for IoT

Modelling target type	Modelling language	Modelling features covered
sensors and sensor systems	OpenGIS.® Sensor Model Language Encoding Standard (SensorML) [96]	Management and inventory of sensor and sensor systems, observation and resource discovery, observations processing and analysis, performance characteristics, explicit description of the process, archive fundamental properties and assumptions, hardware description and many more.
Context	OMA NGSI Context API-Next Generation Service Interface (NGSI), the Open Mobile Alliance (OMA) [97]	Context Source Management includes registration and discovery of context sources, Context Information Management includes update, query, and subscription operations.
Business Process modelling	Business Model and Notation (BPMN) 2.0 [98]	Model Exchange between various tools by different organizations including the graphical process information, and new forms of events and event dependent sub-processes.
Service	Service oriented architecture Modelling Language SoAML [99]	Pervasive Services, including Enterprise necessities such as Directory Services, Transactions, Security, and Event handling (Notification). The Domain Facilities, in industries such as Healthcare, Manufacturing, Telecommunications, Biotechnology, and others;
Semantic annotation of WSDL Web Services	W3C‘s Semantic Annotations for WSDL (SAWSDL)[100]	Allows referencing of semantic model concepts by WSDL components as annotations.
Sensor modelling	SSN W3C Ontology [101]	Models the sensor from device, process, and system point of views, and includes different operational, device related and quality of information attributes that are related to sensing devices.
Standardization activity		
IEEE 1451 [102]	Documents and services enable the interaction with heterogeneous systems.	
ANSI N42.42 [103]	Provides XML based data interchange format for Homeland security radiation services irrespective of their manufacturers.	
Common Chemical, Biological, Radiological, Nuclear CBRN - Sensor Interface (CCSI) [104]	Provides standards for CBRN sensors interoperability, net centric operations, and basic command set control, XML communication, power, sensor installation, sensor power, sensor communications, sensor operation, sensor environments, and sensor security and many more.	
OGC sensor description standards [105]	Observations and Measurements Schema (O&M), Sensor Observation Service (SOS) ,Sensor Planning Service (SPS) , Sensor Alert Service (SAS) , Web Notification Service (WNS) , Sensor Model Language (Sensor ML)	

2.8.4 Analysis –IoT modeling techniques will vary as per output requirements, and data type of any application. None of the above projects has described the features for all data types (audio, video, image, data, etc.) in IoT aware business processes. As per output, the requirements can be error reduction, security etc, and will vary with physical or virtual Things. As per the output requirement, the modeling requirement will vary and modeling can be done with UML and new Business Process Execution Language (BPEL)- both languages. The modeling language should be able to model process dynamically as per the environmental atmospheric changes. XML and extended XML languages can be applied for IoT modeling. Stand alone applications and the web based IoT application process model requirements are different. Languages should support conversion from standalone to web models and vice versa. I. e model should be semantic. Plug and play provisions shall be available in process modeling languages.

Conclusion can be drawn that at present no modeling language is supporting all the requirements of a dynamic modeling language. It is under development.

2.9 Open Issues and Challenges

2.9.1 Architecture

There is no concrete generic IoT system reference architecture model available yet. There are many perspectives to be addressed. Scalability is one of the perspectives and plays a major role in architecture design. Scalability in terms of data, services, and devices, searching and storing techniques shall be addressed. **Chapter three proposes and proves logic for the scalability of data at source leading to fulfillment of concrete generic IoT architecture along with many other advantages.** As per the development of IoT, new infrastructure and services may come into the picture. Present hardware, resources and software may not be able to scale for accommodating new services. The problems can be like, number of devices requesting a service from the IoT infrastructure. Very large resource entries in the registry of an infrastructure services, may result in time delays or malfunction. Client device resources become constrained towards periphery. The resources can be bandwidth, battery, and processing power. With these constrained resources, it is difficult to make entries in their registry, and search for the service fast.

Interoperability perspective is another major issue of an IoT. **Communication technologies Wi-Fi, Bluetooth and Zigbee co-existence can be thought of as one of the ways for HI and based on the co-existence same concepts network architecture is proposed in chapter four.** Service oriented architecture shall take into account the semantic interoperability. Events generated shall be enhanced with the help of context generated due to semantic interoperability. Considerable Research is required to be done for getting an automatic interpretation of events along with semantic annotations for answering why, and when events have occurred. What measures need to be taken further? Research is required to be done in vertical domain cantered business vocabularies, semantic web based ontology (specification of a conceptualization), and semantic mediators. The research can be focused on dynamic SOA based business processes. The features like reference architecture and protocol suits, identification schemes, routing and addressing, resource resolution and lookup, and semantics should be considered for interoperability research.

Things are scattered in a decentralized and heterogeneous manner. They interact with other entities trough resources, which can be again decentralized and heterogeneous. For completing the requirements of such cases, architecture should be scalable, flexible, open layered, and event driven. Till date, there is not a single programming language, operating system, and an information transport mechanism available yet, which takes into account

heterogeneity. Because of resource constraints, there is a need for research on caching and synchronization updates between two communicating things, where reliable permanent connectivity is not available. The implementation of cloud computing technology for Things related services can be a good area of research.

2.9.2 Communication Technology

Information exchange between two Things is based on communication, network, and network discovery technology. Communication technology has many perspectives such as deployment, mobility, heterogeneity, communication modality, infrastructure, network topology, coverage, connectivity, network size, lifetime, cost, and energy required. This points that, no single hardware and software platform will be able to support the communication. Multi frequency radio front ends for the communication spectrum and frequency allocation, software defined radios, cognitive radios, and inter protocol communication technologies are some of the issues considering the above perspectives. Software defined radios remove the need for hardware upgradation when a new protocol emerges. Connectionless communications beyond IP are required to be researched. Network technology finds visions to connect two things in a network. Solutions shall allow connecting anything to the network with reduced costs, which in turn will affect the information processing. Network on chip technology for on chip communication architecture, which allows virtual connections, scalable on chip communication infrastructure for varying loads or constraints and a network of networks are the areas of research. Power aware, all types of networks are expected, which turns on and off their links as per the requirements.

Data collection in these networks [11] is a primary issue. Networking technologies like RFID, active and passive RFID networks, WSN, mobile connectivity has lots of issues in turn. RFID data is extremely noisy, redundant, and incomplete. RFID range increments, sensing more detailed information is required to be worked for getting better data and reducing reading failures. This leads to repeated scan of EPC tags at the same location by multiple readers generating huge data and can lead to numerous challenges from data perspectives. These tags have considerable privacy challenges. The major challenge is to clean the missing data collected in such way. Many methods are available for cleaning data [106-108]. Active RFID's battery life is limited by IP protocols implemented for internet connectivity. They need to keep on, continuously for connectivity leading to battery life as a significant challenge. Such collected and cleaned data also has quality issues because of voltage conversions and other noise.

Things, network infrastructure, and resources are heterogeneous and can be placed at different locations. Underlying data in such scenarios is extremely large, heterogeneous, and noisy. It is a major challenge from the data analysis point of view and storage. Semantic interoperability challenge is an extension of such interoperable data. Data- centric standards are required here, for homogeneous interpretation of heterogeneous data. Linked sensor data has two more challenges. First, is to establish the meaningful link between these data sets like observations, sensors, features of interest, and observed properties. Second, is to refer to the changing and frequently updated data sets using Uniform Resource Identifiers. There are lots of data mining and warehousing challenges to be addressed.

IoT is the beginning of a data centric web. Search functionality will be extremely challenging as the size of the web is several orders of magnitude greater than the conventional web. This further poses challenges for crawling, indexing, and retrieving results from the web. Data scalability and all related function executions along with storage issues are an enormous challenge.

2.9.3. Software - Hardware

Hardware for network and objects/Things is manageable only with the help of software. Distributed intelligent (self configuration and auto recovery) software is available. Software for virtualization, object interaction language, bio inspired algorithms, algorithms for optimal assignment of resources, and mathematical models for inventory management and data mining are some of the software issues.

Research and development is required in field processing gate arrays (FPGA) hardware, which changes its configurations as per context, dynamic very large scale integration (VLSI) circuits containing scalable cognitive hardware. Along with it tamper resistant technology, miniaturization of hardware i.e. nano technologies, embedded sensors, and actuators are required to be worked further. Spintronics (magneto electronics), micro-energy microprocessors and microcontrollers, and energy efficient RF front ends are the important areas for research.

A meme acts as a unit for carrying ideas, symbols, or practices that can be transmitted from one Thing to another through writing, speech, gestures, rituals, or other imitable phenomena. The concept regarding memes as cultural analogues to genes of Things in that they self-replicate, mutate, and respond to selective pressures. Meme needs research with software and hardware ends. This will create the relationship between the various networks.

2.9.4. Power and energy storage technologies

Energy storage is one of the obstacles in miniaturization of embedded electronic devices of wireless technology. It is very much required to find the miniature high storage technology. Harvesting of energy in all possible ways is needed to be worked. It should consider electrostatic, piezoelectric, and electromagnetic, photovoltaic, wireless energy transmission schemes. Micro power ICs and transducers, micro battery technologies, micro fuel cells and reactors, and micro combustion engines for power generation can be challenging areas of research. Super capacitor technologies for energy storage have to be found out and will be helpful in miniature storage means. Wireless transmission of energy and energy compression techniques can be different areas than usual.

2.9.5. Privacy and Security

Privacy and confidentiality of data comes under this head primarily. Wireless communication is persued more and more now days. Air is shared as a physical medium by all nodes. Attackers can easily and anonymously access the packets in the air. Heterogeneity and mobility of things pose more security problems. If proper security care is not taken, data can be accessed very easily. In IoT as devices are constrained in computing or processing power, taking strong security measures is a challenge. I.e. the encryption keys are smaller, which can be decrypted very easily. There is a need of privacy preserving technology for the heterogeneous state of devices, and technologies for object and network authentication. **Chapter five proposes and proves co-operative all types of grey hole detection algorithms as an example of DoS attack. An algorithm helps in authenticating the foreign nodes.** Security scenarios like hop-by hop, in constrained and unconstrained networks through gateways, collaborative end-to-end security, and server assisted group security for constrained devices shall be studied more. Data ownership is a major issue in security in general and in cloud computing. Security and trust for cloud computing is another research area under security.

There are no physical authentication means available or possible with wireless communication. Malicious users can inject forged packets at the Link Layer creating problems in the functionality of upper layers. Confidentiality, integrity, and authentication features for peripheral networks can be achieved with security frameworks at the Link layer. The same will protect the functionality of the upper layers. In such networks, there is no trusted device or actor, which may lead to destruction of the complete network.

The security framework should be developed independent of the communication stack. This should include knowledge of its own devices as a static profile, bootstrapping and

authentication, and collaborative security action management when node capabilities are not sufficient to handle the attack. It can have security level imprinting on packets group security and many more blocks the security of embedded devices and can be improved with the help of proxy situated near devices.

2.9.6 STANDARDIZATION

Standardization should take into account requirements from industry, environments, society, and citizens in all aspects. Many fields are open for the standardization of IoT from its own definition, semantic ontology, bidirectional communication, and information exchange standards in all conditions, energy and network capacity standards, standards for communication within and outside the cloud. It should also take into account the constraints of existing standards and reform new ones. Various frequency bands, wireless internet, short rage radio, and frequency band allocations are also not standardized the same in all the regions of the world. There is a big chain of challenges of standardization from very small things to communication technology. All aspects of hardware and software of business process, internet, and physical or virtual Things, are areas of research under standardization.

2.10. Conclusions

This chapter has endeavoured for IoT definition and indirectly IoT architecture requirements. As per definition it is brought to notice that how some points are missed out for developing concrete generic IoT architecture. The chapter two is worthwhile for finding state of the art, challenges, issues, research areas, as well as information for the development of IoT software or hardware applications / projects. The chapter bridges a detailed and focused IoT state of the art to the readers. Some IoT perspectives themselves are very huge and will form a framework.

Architecture: -IoT Definition standardization will lead to focused efforts towards concrete reference architecture. Efforts for concrete architecture development will provide many new inputs of all perspectives along with modelling language leading to good progress in all aspects. Object naming server allots a name to the objects, but after the expiry of these objects, no research efforts are seen.

Protocols: - For stationary non remote Things connectivity to the Internet is not a problem. But with mobility of Things protocols need to be tested for a number of scenarios. Examples can be food, medicine, and other products, which keep on moving from one place to another. Heterogeneous communication should be made possible with constrained devices.

Security: - It is a combination of legacy Internet and emerging peripheral constrained Thing's security and privacy. Privacy of individual's information is on the highest priority, or else it may create problems in day to day life. Ubiquitous and pervasive nature of IoT is going to create vulnerabilities as per location and need to be tackled separately.

Platforms and OS:-There seem to be limited manufacturers for hardware chips. Dominant technologies are Zigbee and Bluetooth. Contiki OS seems to be ideal for constrained devices.

IoT modelling: -Application development can have a single Thing, network or web for it. The effect of the dynamic nature of an individual Thing, network, and web on each other for any application can be studied with the help of process modelling. As per data of an IoT application, and output requirements modelling techniques have to be developed. Modelling techniques shall provide real environmental situation effects on Thing, network, and the web.

Challenges: -From Challenges and issues we can say that IoT is a multidisciplinary umbrella. Investigations are helpful to all discipline readers for research. Researchers can contribute in standardization bodies' activities.

General: -There can be a major challenge of e-waste of these Things in future. Tabular state of the art helps in reading fast, the huge IoT domain's state of the art. Governance of intermediate things is also an open issue. There are still some technologies, which are not covered like data and signal processing technology, software and algorithm technology, and relationship network management technology in the chapter to a full extent.

Finally, purpose of the Chapter is served to analyze existing information in theoretical way.

Chapter 3

Internet of Things System Reference architecture Design

3.1 Introduction

The literature survey in chapter two concludes that there is a need of IoT generic architecture. Conclusion is taken further as a research objective for this thesis. Generic architecture should characterize a whole group of features with past, present, and future IoT architecture requirements. IoT architecture design is very huge research and required to be designed by thousands of people. Thesis has worked for abstract architecture design, for the same reason. Internet of Things (IoT) is characterized by ubiquitous, pervasive, and seamless networks. Keeping functional and non functional characteristics in mind, the features and requirements of generic architecture have been found out. Chapter explains various types of things and their properties. This chapter contributes in software architecture, abstract generic IoT system reference architecture and architecture for scalability perspective.

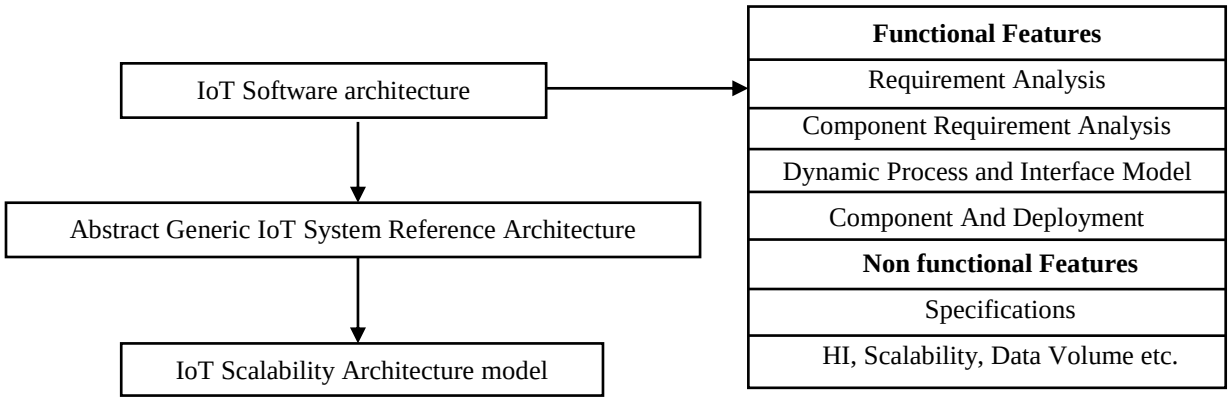


Figure 3.1. chapter flow diagram

Section one outlines the chapter flow graphically (ref fig. 3.1) and overviews section wise contributions done for IoT architecture. Thing is one of the basic part of IoT without which IoT is not possible, and is explained in section one. Section two contributes in design of software architecture. Section covers functional and non functional features. Individual actions by each of the components in package, its deployment on hardware and qualities of a complete system becomes clear in this section. Issues and challenges, as an outcome of requirement analysis are explained in section three. These issues and challenges can be valuable for researchers. Abstract generic IoT system reference architecture is proposed in section four which is one of our objectives. Section five illustrates limitations of the verification and validation process of architecture. Scalability as a first non functional requirement of IoT architecture is worked further. Section six proposes IoT scalability architecture model. Section also provides solution for architecture scalability. Proposed concept is simulated in paper [109]. Various IoT applications considering daily requisites at

all levels from individual to country are mentioned in section seven. However, the scope and the list of applications are not limited. Conclusions are given in the last section eight.

Section two, three, four, five, seven and eight are contributed by author. Section six just outlines or gives scope of the IoT applications. Proposed architecture will direct or provide a ground work for entrepreneurs, researchers to manage any IoT architecture in better way. They can design and implement directly IoT architecture at process level. Scalability solution will be extremely useful, in almost all IoT applications.

3.1.2 Things and their properties

Objects or Things have a key role in IoT. It is important that, we define what we mean by things or object in context of IoT. We need to clearly understand, what are the properties of the things, their capabilities, and limitations.

The concept of the thing in IoT is that, it may communicate information of interest, record, and process potentially any time, any place, and to anyone, when needed [107].The information can be made available by a single node or a number of nodes in a group. When the information is available through some physical thing or object, we call it a physical thing i.e. RFIDs, sensor nodes, motes, actuators, bar codes, all could be example of things. Fridge, TV, Laptop, temperature of a room, and humidity in an atmosphere are some examples of physical things.

There are various types of things available with IoT. But word "Thing" is applied as general term to represent all. Things can be static or dynamic. This classification is based on the type of power source used by things. When battery is recharged by some external means, it is dynamic. If it is using permanent battery, it will be static. Millions or even billions of such physical things are expected to be connected with Internet, and then monitored or controlled, and therefore the concept called as Internet of things.

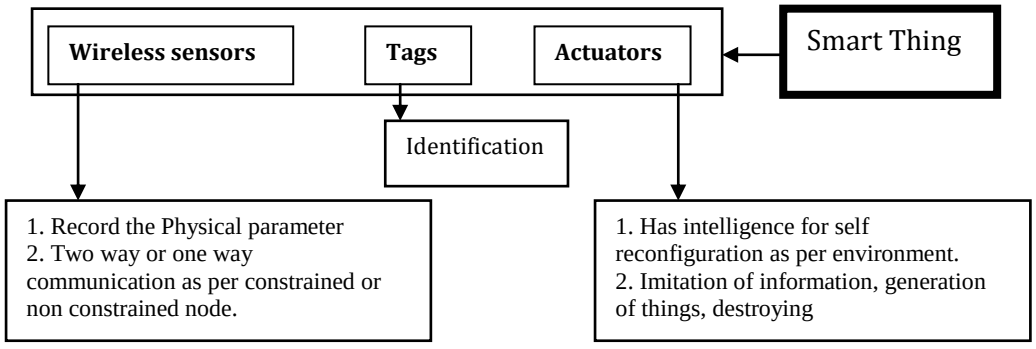


Fig 3.2: A conceptual representation of a Smart Thing/object.

To uniquely identify it is necessary that, each object has some sort of identity. The identity to thing/object can be assigned by a unique number, or a code, or a name, or combination of these. Moreover, things have life cycles of different durations. They can be either damaged due to the environment or end of its use cycle.

Things are also called "smart things". The terminology of "smart things" is developed independently. Although there is no precise definition of "smart" in smart things. There is not even a way to measure what level of smartness such devices yield. However, smart thing is rather a concept where things have some minimum level of functionality, such as changing the parameter under observation as per smartness. Wireless sensors with tags represent physical things and physical things with actuators represent a smart physical thing. Figure 3.2 represents a smart thing. An actuator controls the parameter. An actuator can be called as an agent. The agent can be an artificial intelligent agent or any other autonomous being. An actuator can be a moving or stationary robot, which has the required intelligence for taking decisions and setting the environment accordingly, as per the application of the environment. Sensors sink data from the environment to measure the state of an environment. Actuators source the data to the environment to set its state. The properties of a smart thing are mentioned below and are possible due to actuators along with sensor nodes.

Things can interact with things and people and vice versa. Things may operate individually, or in a group forming a network. E.g. environment's physical data can be represented by a single thing, but other Meta information has to be represented in a group. It can imitate information and while doing so, it manipulates the required resources and services. They can do many tasks autonomously. It can sense, record, process, communicate, move, and maintain its own privacy and security. They have the decision making capability, self awareness, and limited intelligence. It takes care of its own life with power monitoring, saving, wastage, and the availability of power. Things can create, manage, and destroy other things i.e. Physical things can generate or destroy other Things. When edge technology has the intelligence to add many smart automatic reconfigurable properties mentioned above for things, it is a smart thing. E.g. RFID with actuators, sensors with actuators.

3.2 Proposed IoT Software Architecture –UML Diagrams

As architecture design is at an abstract level, only the major modelling diagrams are displayed for static (structural) and dynamic (behaviour) views of IoT. Static view of IoT is represented by a component and deployment diagram. The requirement analysis is completed in such a way that, it is a collection of various components and when clubbed together can be

formed as a package. The IoT Behaviour view is united with the sequence (Dynamic process) and Interface diagram. It states the essentials of individual components or packages for data flow with a ball and socket diagram. The number is also put up on a sequence of events, which occurs, when the user wants to connect to a Thing or vice versa.

3.2.1 Functional Requirement Analysis

Requirement analysis is the first stage in the systems engineering process and software development process. The requirement model contains the functional and non-functional requirements. The functional requirement offers a behavioural analysis for the system. The non functional requirements impose constraints on the design or implementation (such as performance requirements, quality standards, or design constraints). Our focus is on developing the core architecture for IoT. Looking at the research-done for IoT, by various EU applications, projects and analysis of IoT applications have put forward the various functional requirements [110-114] of IoT architecture. This analysis helps to yield the basic generic architecture for IoT.

3.2.1.1. Functional requirements

They define behaviour of a system or indirectly of components. This behaviour is dependent on set of inputs and outputs. Following discussed functional requirements must be done by the proposed IoT architecture.

3.2.1.1.1. Component diagram

The minimum compulsory software components in any IoT application required are found out and shown in figure 3.3. According to the execution process sequence and the corresponding requirements, the components (all entries below individual package) are placed under package in the diagram. There are three major packages as user, Internetwork and Thing. Package names are given, so that anyone can find the place of the component in IoT as well as visualize, functionality required to be provided by each package at that place. Various component names under all packages, indicates behaviour by that component. The word user is a package name with various components listed, in that package. User package represents all tasks which are supposed to be done at the user application side. User can have various devises like mobile, laptop, PDA etc. In the similar way Internetwork and Thing package names are followed in proposed software architecture. Proposed software architecture is generic and is able to support any IoT application execution.

These major packages can be at different locations and their software components need to take care of linking all these blocks along with the hardware. Event manager, Filter manager,

security, power controller, and local database storage are some of the components present at all the major packages of IoT i.e. at user, Thing, and at Internetwork packages. Even though component's names are same, they will take care of all the requirements at the corresponding package place.

Package Things: Various types of Things are available. They are very small in size (shoebox size to a grain of dust) and costs very less. This leads to limitation on computing power and resources on them. The hardware abstraction layer takes care of recognizing all these devices meant for reading the various Things. These devices shall be read even if they are not standardized, and plug and play sensors logic is required for connecting these devices. When things are read, authentication and authorization plays an important role of security. After authentication, the information read is filtered and the events are generated. Thing reader devices read from things, and events are generated and stored at local (at reader or at Things network level) and centralized databases.

Package Internet: It can have a single or any combination of networks as displayed in figure 3.3. The IoT Internetwork can be considered as a global network [115] with a core and peripheral networks. Things networks are peripheral networks and can have heterogeneous network technologies, and different scenarios. Different protocols will be required as per type of network technology and scenario. Each network will fulfil its own QoS and applications QoS requirements. Internet is formed, when all of the above networks exchange information with each other using TCP/IP. Generated events with contexts from databases will be operated to achieve the required QoS. Self awareness is an important feature expected for an Internet. As an example paper [116] plays a role of taking precautionary actions in catastrophic situations as a self awareness.

For rural and catastrophic areas one of the features for internetwork is connectivity with fast, easy and economical network erection. Chapter seven provides solution as a first aid for these areas. This can be considered as an internetwork of handy cam and LED towers for rural and catastrophic areas

Component Servers: The internet provides information and services through servers and clients. Cloud computing serves server to server grid communication. Each and every physical or virtual Thing must have a unique name, which is obtained from an object naming server. The Death report Server is required for providing the information of Things after its death. Filter, events, security information, death report, and Object Naming Server (ONS), databases play a very important role. Other than these, there will be many other servers for different routine services like backup, emails, prints, etc. Information-data generated by

objects/things or various applications will be read by the user through servers. Proper technology has to be selected for storing, retrieving the same data.

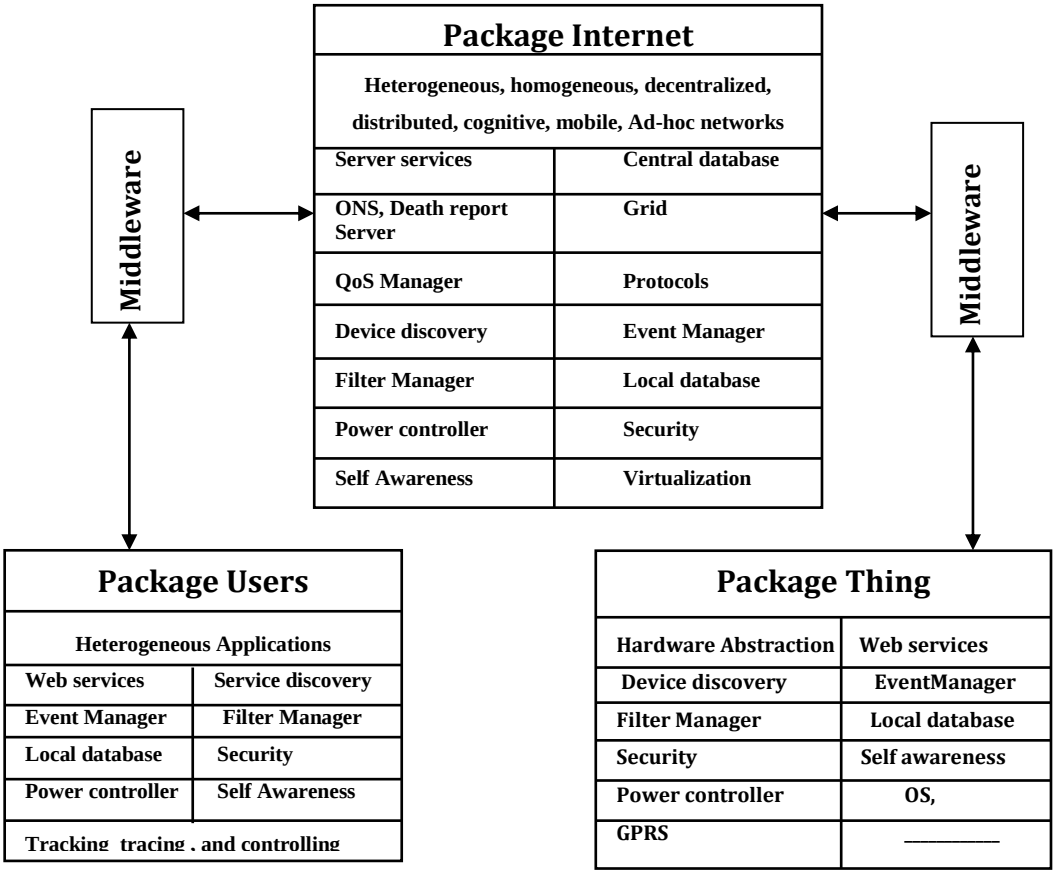


Fig 3.3: IoT software reference architecture components requirement block diagram [116-120]

Package Users: User can be interfaced to Things with various means like laptops, mobiles, PDAs, etc. through corresponding applications (business processes). These users (applications and devices) through web services are connected to Things. Services from user to server and then from server to things or vice versa are required to be executed. Here two heterogeneous environments are present. To handle such heterogeneous environments middleware is required. Middleware is an abstraction layer (software component) that hides details about hardware devices or other software from an application. E.g. service discovery request from user to server and then server to thing uses http (user to server or vice versa) and CoAP (Server to Thing or vice versa) transport protocols. So conversion from http to COAP and vice versa is done by middleware.

IoT architecture has event generated functions as special feature. Various applications generate many outputs or results, which may create events. Events are filtered according to

criteria's. These events further activate predefined functions. These functions can be based on different contexts from the databases. While executing various applications, the output of one application can be directed for another application. When such results are required to be handled from various applications, middleware comes into the picture. It may convert data formats from one application to another. Security as well as privacy is important in such cases. As billions of things shall be connected, the discovery of services becomes an important component of this block. Special components shall be headed to reduce power consumption.

3.2.1.1.2 Dynamic process and Interface model

Dynamic process is represented by a data flow diagram. Sequence diagrams are structured to display the interaction between users, objects, and entities within the system. It provides a sequential map of the data passing between objects. We identify and propose the requirement of a number of interfaces from object to server, user to server, and vice versa and between the various applications. The integrated dynamic process with sequences and interfaces for IoT architecture at an abstract level (Each component functions can have number of sub components research hierarchy under it.) is proposed and visible in figure 3.4. Total three layers are explained as user, Internet and Things (L1, L2, and L3 respectively). At all layers we see same component names, but their functions varies as per layers. At each layer a local database is present. Query to Thing will be transferred through the internet with heterogeneous networks and components. Else through the respective component and then HI component. Thing will answer to the user through the server only. Remote method invocation or Common Object Request Broker Architecture (CORBA) plays a major role in accessing the information of remote objects. CORBA is more advantageous in the portability of objects information. It is independent of programming languages as well as platforms. Total of 20 interfaces are in the diagram except the applications. Any two objects from different layers may require information from each other, using individual interfaces (e.g. L1 to L2 and vice versa). All such interfaces are on the same line with ball socket symbol for each. User, Servers and things are required to read and write information from each other for some specific tasks. Accordingly, these interfaces are displayed and the names are given. Numbers wrote on top side indicate the execution process sequence steps from the user to the server or vice versa through middleware or through HI component. The bottom side number represents Thing / objects to the server or vice versa and interfaces through middleware or through HI component.

- Interfaces in user to Thing communication – application components communicate to any of the servers or databases (L1-L2, or can ask to Things L1-L3) directly. In this process of communication all related interfaces will be implemented as per requirement.
- Information can be relayed for local or remote distributed applications. The application may generate new things along with query or data. I.e. Things can be at user package side as well as Thing package side also. That's why all the components that are indicated on a things layer are also present at user layer along with applications. The new thing related data shall be filtered, and can generate an event, and can be stored on a local or server data base. Interfaces like filtering, event management, object naming component (ONC), and security components will play a major role, and finally, the information will be stored locally as well at the server database.

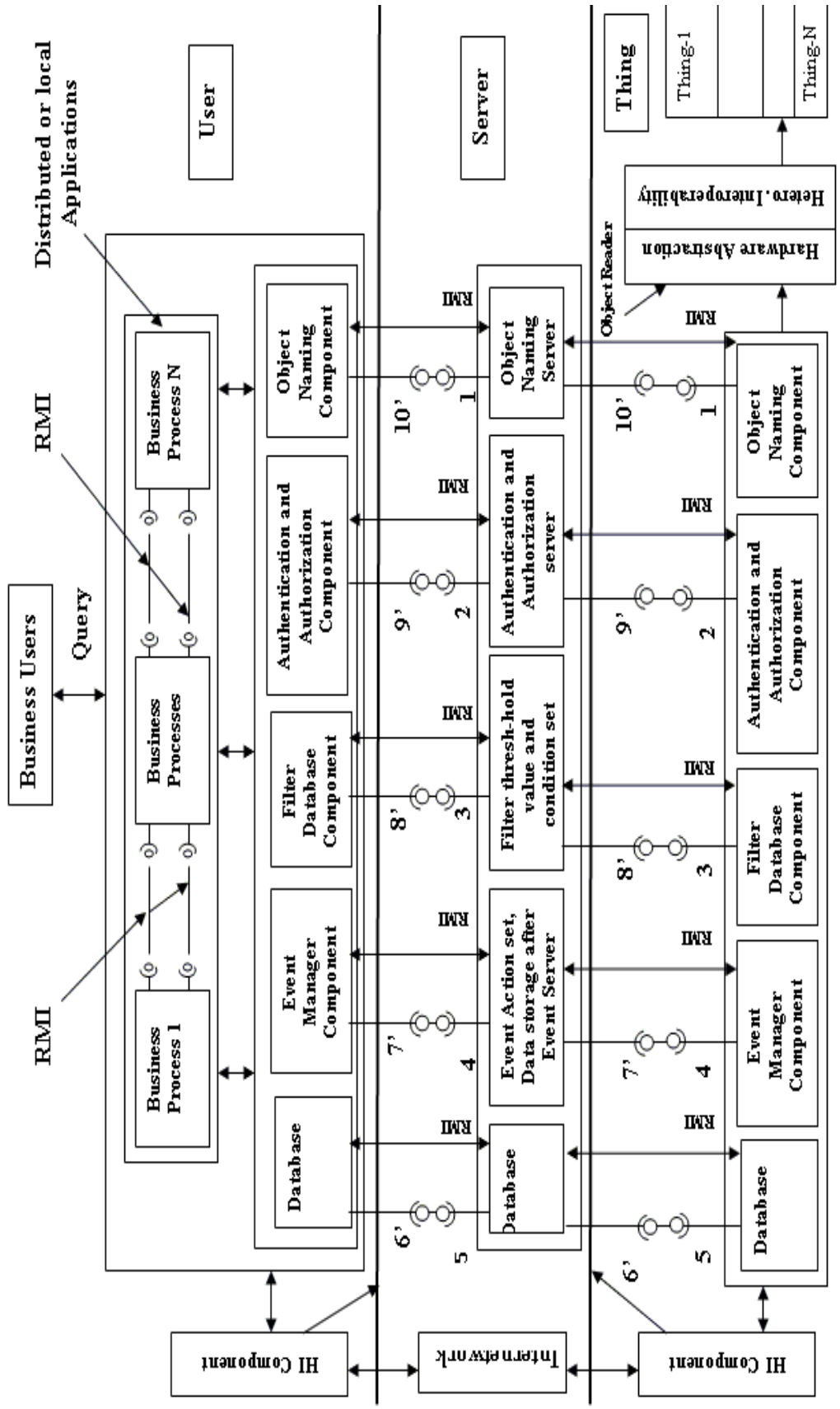


Fig 3.4. IoT Architecture - Dynamic Process and Interface diagram

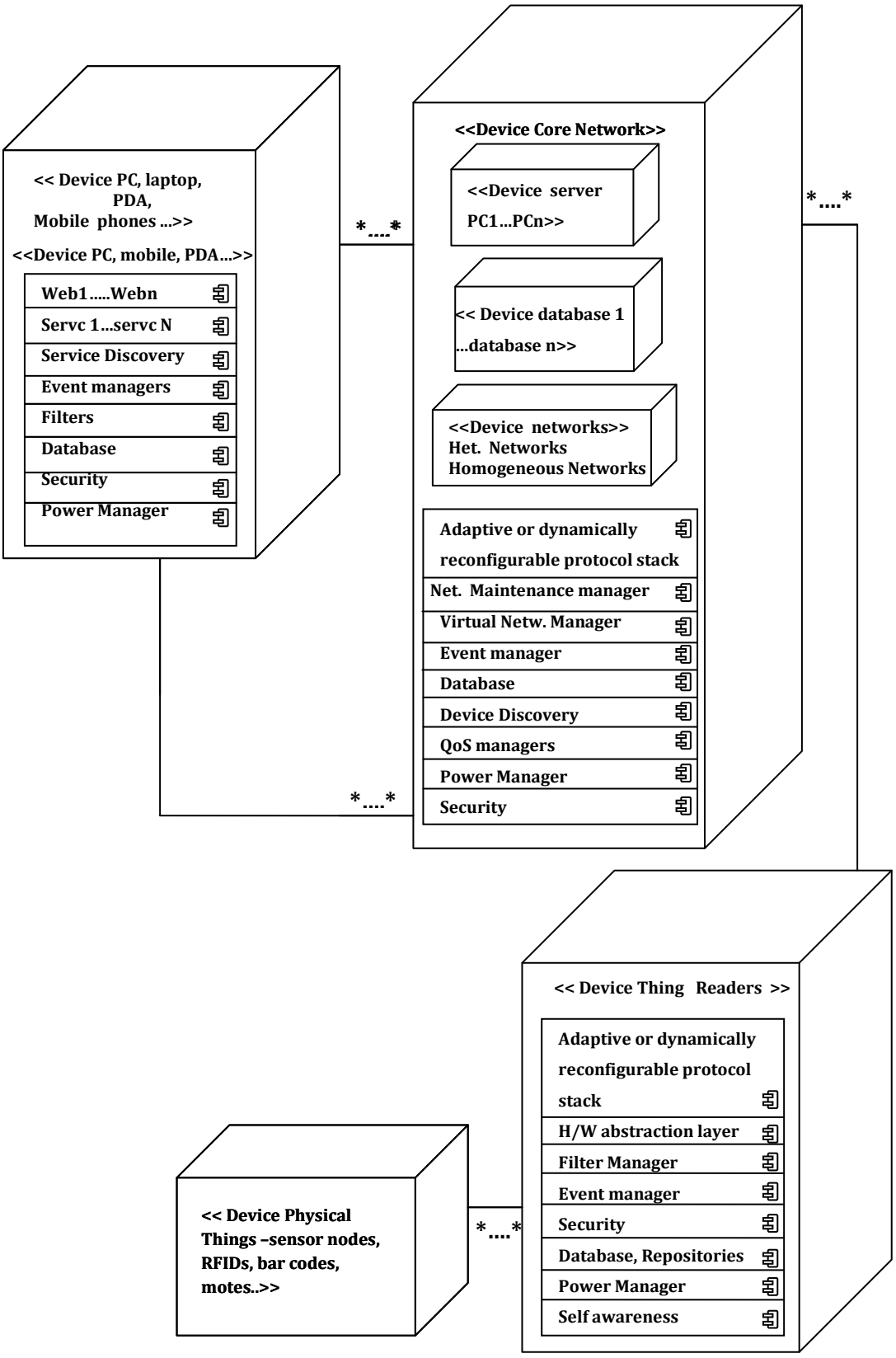


Fig 3.5: IoT Deployment and Component diagram

3.2.1.1.3. Component and Deployment Diagram

Component diagrams are structured to describe the software components and a deployment diagram helps to visualize the hardware topology of a system. Component diagrams and deployment diagrams are closely related and traced in figure 3.5. A deployment diagram specifie the various physical devices in an architecture on which, the software components are executed. The diagram is at an abstract level . Each major block can have number of hardware options. These possiblities are mentioned here. The first major block is of User package. Hardware for users allows to interact with Things through Internetwork. The user's or client's devices can be a PC, Laptop, PDA, or mobile phones with a web support on it.

Second major block is package Internet and requires to handle servers, gateways and every other infrastructure required for networking. Hardware infrastructure related with Internet has variety of servers and network related hardware. Server devices can be of various types like Hp-UX, Linux, Sun, Object Naming Server, Solaris, Windows, z/OS, Advanced copy services, databases, Enterprise Resource planning, Mail, System Backup and Recovery, Archive Manager, and many more. A core network can have base stations, wired and wireless links, routers, bridges, power supplies, and many other devices. The adaptive or dynamic protocol stack is the connecting device between the core network and peripheral network or and any two heterogeneous networks. Present Gateways will be part of Internetwork. Data Gateways are the most suitable for helping data transfer from one network to another network. Home gateways or Multimedia gateways also can be placed as per the requirement. The core network block is indicated as a single deployment device instead of separate ones along with the components in them. Filters, Event managers, power consumption, database, and security components are present at Things, users, and internetwork places as denoted in figure 3.5. All these components will have different ways of implementation functionalities as per the places where they are.

At package Thing side any type of physical thing (as covered in 3.1.2) can be present. The hardware devices can be RFIDs, motes, sensors actuators etc. As the diagram is at an abstract level * ...* (many to many) association is marked. They represent a relationship between objects. Associations refer to the role and the multiplicity of each of the participants. Multiplicity is displayed as a range [min..max] of non-negative values, with a star (*) on the maximum side representing infinite.

3.2.1.2. Non functional requirements

3.2.1.2.1. Specifications

Requirement analysis formulates some of the architecture specifications and displayed in table 3.1. These specifications are based on existing and legacy systems in IoT. Design of each component under all packages will offer exact specification. Unless and until the methodologies for all the components are finalized, it is difficult to present all accurate specifications. As architecture design itself it is at abstract level, mentioned specifications are applicable to abstract level.

Table 3.1 : IoT Architecture Specifications

<table>
<tr>
<td>Thing (Physical)
1. Size :- <= few square mm
2. Capability – All properties covered in 3.1.2
3. Power consumption – mW- nW</td>
<td rowspan="2">Network
4. Bandwidth – As per Radio waves, X rays, y rays, UV, visible spectrum, IR microwave etc. (unlicensed band 2.4 GHz)
5. Address space- IPv6
6. No of things - 50 to 100 trillion objects Communication type- Unicast, multicast, Broadcast and many more covered in chapter two.
7. N/w Technologies between Things – Smart Bluetooth and Zigbee, Eterna™ 802.15.4 SoC, wireless HART , Ethernet, 6LoWPAN etc, Technologies with mobility of nodes</td>
</tr>
<tr>
<td>Thing resources
8. Microcontroller data bus – 1 bit to 32 bit
9. ROM - few kilobits to a few hundreds of kilobits
10. Frequency – few KHz to few THz (300 MHz, 868 MHz and 2.4 GHz, ISM frequency bands)
11. Microcontroller size – Ultra small (e.g.1.9mm * 2.mm e.g. Kinetis KL02) or few square mm
12. Battery life – few days, 100+ Yrs or more
13. Battery size – micro electro mechanical systems (MEMS), mm to nm.
14. OS- contiki, TinyOS, RTOS along with core network OS etc</td>
</tr>
<tr>
<td>Software components
1. All components as shown in the figure 3.2

HI
Data, Services, Networks etc</td>
<td>Data volume
1. Bigger than Big Data

Security
1. Privacy, confidentiality, availability and Integrity

Hardware components
15. client’s devices - PC, Laptop, or PDA, mobile phones
16. Server - Object Naming, Death Report, Database and many other ...
17. Gateways -Data, Home or Multimedia</td>
</tr>
</table>

As per future requirements, there can be addition or deletion of these specifications. There is a requirement of adopting things, resources of things, and Networks (everything related with network) with any specification in case of an ideal implementation IoT. E.g. non standardized things are also expected to be connected to IoT. Taking into consideration all above limitations and facts of generic architecture requirement, specifications are put up.

3.2.1.2.2. Other non- functional features

For abstract generic IoT system reference architecture to be concrete, it should take into account the non functional features like scalability, security and privacy, data volumes, device adaptability, interoperability, power consumption, self awareness, and discovery mechanisms in advance. Taking these features into consideration in advance will, make the architecture more efficient, economical, and accurate. Figure 3.8 explains the proposed architecture. All these features themselves have a huge framework. The importance of the features is explained briefly.

a. Scalability - Scalability can be horizontal and vertical. For horizontal scalability some authors have suggested that IoT can be implemented as a human nervous [121] system. The network size of a normal computer network or telecommunication network will be too small in front of the IoT network. Scalability in terms of memory, addressing, computing power, and battery life has to be addressed. Different techniques for horizontal and vertical scalability can be found out.

b. Interoperability - Device and service interoperability [122] shall be on a higher side. If interoperability is not achieved, there will not be any communication between thing-to-thing, human to things, or human to machine. Heterogeneous interoperability [123-24] can be in data, devices, services, OS, and networks or different networks technologies.

c. Discovery Mechanisms- Suitable services for objects and their information should be found out under discovery mechanisms. With the growth of the number of nodes (billions/ trillions), available services along with their infrastructure also increases. It will become difficult to find the proper service from billions/ trillions of node's services. A higher degree of automation is required to reduce human intervention. A large number of service discovery approaches are required to be applied. For example, centralized [125], distributed [126], decentralized [127], syntactical [128], hybrid [129], and semantical [130]. A framework has to be formed to cover all the possible approaches of discovery mechanisms.

d. Data Volume - It is a critical parameter for designing the architecture. A huge amount of data or information will be generated because of the number of objects interaction with each other and the different services. This data may get accumulated day by day. Information storage limitation is on an individual object, centralize data storage means as well as on the network. Objects have a limited memory and processing capability. Data warehousing, data mining for retrival of data, Meta data and other techniques shall be found out.

e. Security and privacy - is ubiquitous as expected in IoT. It has to be accorded top most priority in architecture design. Objects are monitoring and controlling our day to day activity. It is quite possible that this information may be stealed by someone, disturbing the privacy. Objects can be of any size, with many constrains as low memory, low processing and battery power, lack of user interfaces, or at any location, but security [131] comes into the picture without any excuse.

f. Device Adaptability [132] - Objects are moving in heterogeneous environments. These objects will be performing various tasks according to the environment. Objects or networks should be self repairable, self aware, self configurable, self modifying, and self adaptive and self organizing. They should have a reconfigurable feature. These self intelligent features suggest the device adaptation metric.

3.3. Issues and Challenges

Requirement analysis also delivers issues and challenges with individual components. They are put up below. Some of the issues are taken as part of research in further chapters as part of architecture design.

Heterogeneous interoperability

1) Heterogeneity is an important feature of IoT. Heterogeneity is faced at most of the time in IoT. So it is very much important to take into account all challenges of it. Putting all issues is not possible, but efforts are made to highlight few important once. The requirements vary as per application. From the previous research we can see that devices (Things), resources, communication protocols, architectures, addressing styles, modelling techniques, security attacks, and techniques all can be heterogeneous. To deal with these points HI is important.
2) Things will be everywhere at home, city, country, villages, under water, in the sky, farms, and at everyplace possible for monitoring data according to applications. The problem will be faced in providing connectivity to these things, at various locations. As Things have limited computing power and a limitation of size, it has restrictions on interfaces (of various network technologies) and the coverage range available. Restrictions on interfaces will make HI difficult or even may not allow HI to take place. Things may have Bluetooth or Zigbee interface in it. It can be inconvenient to place number of gateways for all Things and networks for having connectivity to the internet. A better way is to implement Wi-Fi interface in such a way that, it will cover a number of PANs or Things networks. I.e. connectivity from the smaller area network to

the bigger area network has to be researched. The Interfaces required for a vertical handoff shall be worked upon.

3) When things are taking a vertical handoff, they undergo heterogeneous network interoperability. Things will be transferring information (say reading of temperature sensor) in the form of messages. When thing is moving from one network to another network of different type (VHO takes place), while sending this information in the form of messages to user or with call to user, call connectivity has to be maintained till call is finished. For this fast switch over of call from first network to second network is required i.e. VHO time shall be very small. In the new network, priority or some provision shall be conferred to attain call request of these constrained nodes and minimize time of handover. Various types of information are sent to the server and the user. It is difficult to send data as per the server platform, or user application requirements. A simple format, which will be common to all, has to be set. E.g. XML writer at Thing side and XML reader at the server or user side. Identification schemes, routing and addressing, resource resolution and lookup, and semantics are some of the topics where heterogeneity is present and satisfactory solutions are not available yet.
4) Things networks are peripheral networks. The numbers of Things networks are going to be very big. The effect of connecting such networks on a core network is needed to be studied. Indirectly, its effect on traffic, and QoS parameters of an application are to be monitored.

Scalability

Scalability can be achieved in two ways. Horizontal scalability is achieved when numbers of nodes connected to network are increased because of increase in infrastructure or without any change in infrastructure. Any process which helps in increasing this number will be a solution for scalability. Vertical scalability is said to be achieved when resources of nodes are increased and made free for achieving better results of any process. Both scalabilities are inter-related with each other. For horizontal scalability, connectivity of a network from a single Thing to networks at the country level has to be pre decided. Readymade options are available like virtualization of networks with the help of software. Other than this, the scope for vertical scalability has to be found out from the micro level. While studying each and every action has to be analysed. E.g. If we try to reduce data for transmission from things (at source specifically) to the server and to the user a huge scalability is achieved in security, power consumption, time of transmission, and data storage. It is expected that in software architecture, packages and components shall be

cohesive and loosely coupled for software architecture scalability. If one package or components has to be changed or removed, the change should be easily carried out.

5) There is a huge increase in number of Things (Trillion/Billion). As Things increase, resources, infrastructure and services related with Things are also increased. Some of the scalability issues in architecture development are like increased number of devices requesting services from IoT infrastructure, and a number of resource entries in the constrained nodes or resources. Per parameter monitoring and big number of web pages are required. How these will be provided and how the searching of these web pages can be carried out is an area of research.
6) The addressing style should be scalable easily. E.g. the IPV4 to IPV6 conversion process. Addressing is one of the big issues of IoT. Currently, IPv4 is replaced by IPv6 128bit address for low power devices. This is a network layer address. A solution is required for mapping a network layer to the data link layer.

Security

7) New software attacks are invented day by day. How can physical attacks be stopped? What encryption method will be utilized for constrained devices? It is a big challenge to provide privacy while giving the required information. Authentication and authorization for IoT is one of the important issues.
8) As per the computing power, and number of bits available, encryption methods shall be found out. Cryptography and signing on embedded devices with small keys is one of the core topics of a security research area.
9) Mobile constrained devices security is also one of the crucial parts of research. Problems are increased with mobility as compared with stationary node.
10) Governance of IoT systems is required. Private and public regulatory frames and defining policies for them are very much required. Security and privacy are the important points in governance. Some IoT applications can be distributed in nature. At these various locations, who is governing the things is very important.
11) As Things are meant for tracking and tracing of data, most of the data movement will be from Thing to the server or to the user. How can provision be made for transferring messages only? Can the same infrastructure be operated for it? These questions have to be studied.

Protocols

12) Protocol layer services should focus research on power saving and memory reducing techniques.

3.4.Abstract Generic IoT System Reference Architecture

All software and hardware requirement analysis assist in design of a system architecture. First part of section proposes a model for IoT process. This model further extended to propose abstract IoT system reference architecture and then abstract generic IoT system reference architecture.

3.4.1. Abstract IoT Model

Before starting with architecture design, we explain, expected meanings of model, abstract, generic and reference in relation with architecture. Abstract architecture summarizes the important points, features of IoT architecture. IoT Model or core network is a preliminary schematic architecture that serves as a plan from which a final architecture is to be made. Model helps further to take into account, its known or inferred properties of IoT architecture. Generic means applicable or referring to a whole class or group of IoT applications. By reference, we mean that, this architecture-will be utilized frequently as source, for developing a concrete architecture. New additions or deletions or corrections can be done in this source architecture to get new reference architecture. Process will continue till concrete architecture is developed.

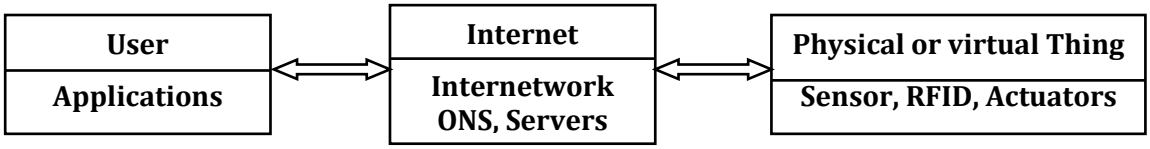


Fig 3.6: Abstract IoT Model

Figure 3.6 represents the general abstract model for Internet of things, having main blocks as users, internetwork, things. Here, model is a preliminary that serves as a platform from which, final reference architecture is to be designed. IoT blocks can be further expanded as per the application's requirements and the architecture is required to fulfil the nature of the essentially autonomous networked structures, that will facilitate interfacing with the physical world, to both collect and deliver information.

3.4.2. Proposed Abstract Generic IoT System Reference Architecture

For tracking, tracing, and controlling, all types of Things have to be connected to the user for some application. Things are small and these constrained devices are connected under peripheral small networks. Things and users can be at same or at different physical locations. To connect them, a core network is required. Peripheral networks are connected to the core heterogeneous networks. So, while transferring data from the peripheral to the core network,

there has to be compatibility of data formats at both ends. To make these conversions meaningful dynamic reconfigurable protocol stacks are required. Information can be sent from physical / virtual Things from the user (application) side and physical/ virtual Things located at various places other than users. The ultimate aim of any information tracking and controlling is to provide some service to the user and is based on these basic steps for the execution of any application. Abstract IoT system Reference architecture is proposed and represented in fig 3.7. Its various blocks are explained below. Gateways are not required as, every node will be able to talk with other heterogeneous node with dynamically reconfigurable protocol stack.

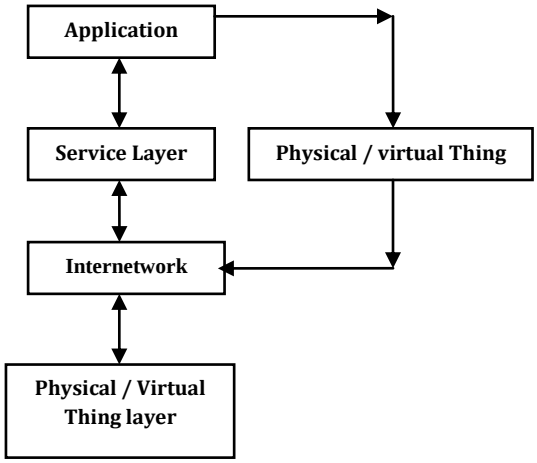


Fig 3.7: Proposed Abstract IoT reference architecture

Things/IoT devices – This layer should be able to connect any physical or virtual Thing to the IoT. Virtual Things can be generated from physical Things and data or the application layer of application objects. A Thing should be able to execute an IP based application. Any standardized [9-10] or non-standardized Things (which are not approved by standardization bodies/ can be below unconstrained things) shall be able to become part of IoT.

Discovery of the devices/ Things can be done with various algorithms. A device, if found to be connected, with the help of UPnP/DLNA technology [120]. It announces the discovered physical devices. Then, the device type is finalized using device ontology and is mapped for device types.

Internetwork – Things can be dynamic in nature. They keep on moving from Bluetooth, to Zigbee, to Wi-Fi, to WiMAX, to UMT or vice versa, or between any two networks Internetwork will have peripheral and core networks. Peripheral network nodes are expected to have dynamically reconfigurable or adaptive protocol stack for heterogeneous

interoperability. Research is in progress for such stacks, which will enable the communication between any two heterogeneous technology nodes. It may act as a middleware for each heterogeneous communication. Traditional communications restrict higher bandwidth, as per networks node hardware capacities. This does not provide optimum throughput of heterogeneous nodes. Paper [133] presents on achieving required QoS quality with Chameleon Java middleware. Paper [134] like previous paper also represents same facts on achieving QoS with dynamically reconfigurable protocol stack.

Paper contributes an architecture and implementation of CORBA [135] base Internet Inter-Orb Protocol. Speciality of architecture is in selection of the elements of protocol stack at runtime, depending on the properties of the interface being accessed.

Generic object oriented model is presented in paper [136] which describes the possible flexible combinations of protocol layers in the stack. Paper has implemented the protocols stack for GPRS, UMTS and IMS access standards.

Service layer – Data from Things is stored on Servers or can be stored locally. The end user shall be able to find out any information and services related with it very easily. Providing service through a web for billions/trillions of things is difficult. Providing every node, internet connectivity requires service repositories, and service orchestration engines for managing service discovery. Some of the examples to provide service to user are mentioned herewith. Discovery of the services at application can generate links to an object and their information resources in turn. Information identified by such links can be highly sensitive for volumes and flow patterns of goods. Authentication and authorization for these services is a key aspect. Security and synchronous responses to queries are the important requirements of discovery services. A layer can apply a synchronous model. Web services and LDAP can be implemented as a search engine and as a repository for searching and storing the directory of the resources respectively.

Application layer - Users shall be able to design their own applications. A number of heterogeneous applications or a single application may be running on the application layer. These nodes as Mobile phones, PDAs, PCs, and Laptops etc will have better computing power. As represented in the architecture block diagram, all the components areas indicated in the figure 3.6 are present on the application layer, at the IoT devices side, service layer, and at the core network layer. The Hidden Markov model can be deployed on the layer for tracking and tracing. A flow pattern along with different contexts helps the user in answering the questions like, the various possible halt locations and movements of objects with respect to the time frame to reach the destination. The model can be further extended with the

probabilistic and non probabilistic analysis [119-120] for various predictions about where an object is now, which path it will select, and where it is likely to be in the future. Applications can be any supply chains e.g. of food, transport, or medicines. Finding the location of objects (say for flight, and how much time is required to reach the destination) may be required in such applications.

All basic important functionalities are covered in the Abstract IoT reference architecture. But to make this architecture generic, it should consider all perspectives which are required along with basic functionalities. The perspectives covered are scalability, device adaptability, Interoperability, energy consumption, security& privacy, data volumes and discovery mechanism (Ref. section 3.2.1.2.2). This complete system represents the Abstract Generic IoT System Reference Architecture and is shown in figure 3.8.

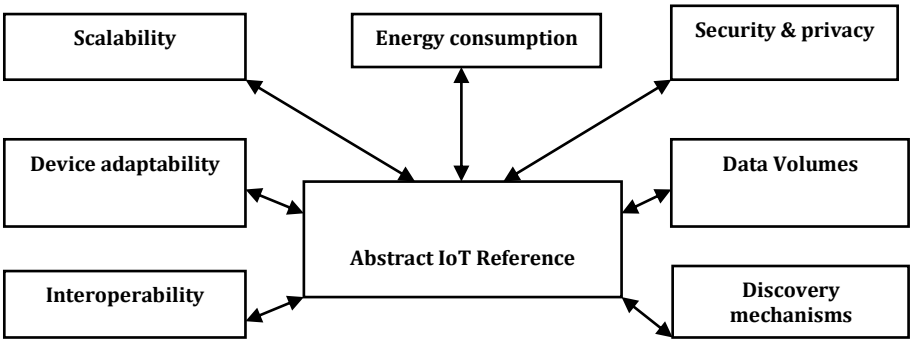


Fig 3.8: Proposed Abstract Generic IoT System Reference Architecture

3.5. Verification and Validation

Validation of a proposed architecture is a next step. Following few paragraphs mention the limitation and outline the validation process for the proposed architecture.

1. Validation is a process of testing and inspecting results. Individual components can become many independent PhD topics, considering IoT architecture software development's huge scope. As there is no code development, making actual verification and validation of it, is impractical at this stage.
2. All sub-components are analysed from required angles of non functional features and then proposed. Architecture components become generic, for any IoT application. These sub components are in working state in many IoT commercial, individual and research projects. So we can say that validation of these sub-components is successful at individual level. Collective working of all sub components as a single component and then package is required to be validated further.

However we suggest following steps for validating our proposed IoT architecture. Each component has to be divided further into small modules. Modules are required to be further divided into various processes. The sequence of validating architecture starts from process testing, and then individual module testing. Further modules shall be combined with individual inputs and outputs connected to each other as per design and then tested. Lastly complete system architecture shall be tested. All the results of testing shall be fed back in correcting the design process. Finally user acceptance test is carried out, which tests system performance, as per user requirements Technical and programmatic risk management is important part of system architecture design. Risk model should be developed along with system architecture. There should be risk management model for various risks. Figure 3.10 displays flow diagram for verification and validation.

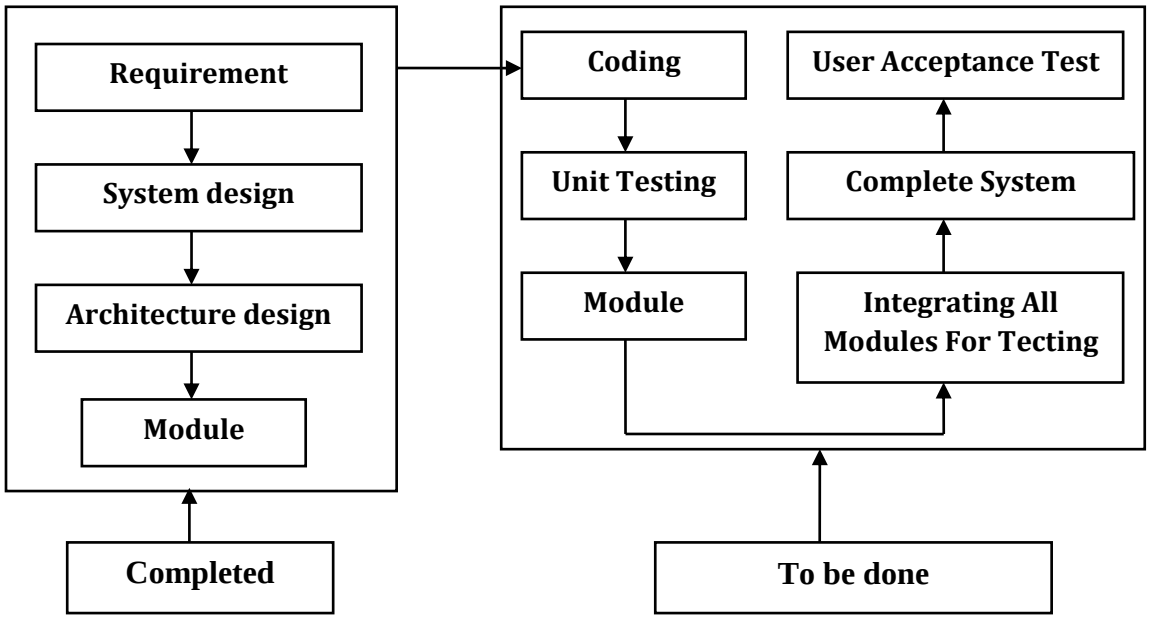


Figure 3.9: Validation Flow Diagram

Verification makes sure that the product is built as per specifications. Validation checks if the specifications are correct as per customer requirements. Testing is expensive and need to be done correctly.

3.5.1. Outline for Verification and validation

Table 3.2 displays the simple outline for Verification and validation. For conducting test of some of this parameter, there can be need for writing separate programs or codes. Tables 3.3, 3.4, and 3.5 list some of the parameters for testing of architecture components, but this list may increase again as per module design and implementation process. Parameter testing may require testing various sub-parameters under it. E.g. input- numbers of inputs as per process,

module or package are being required. All parameters mentioned below, shall be tested for Minimum and maximum number (in thousands, millions, etc.) of inputs and outputs.

Table 3.2: Validation and verification process outline

1. Validation and verification process 1.1 Verification methods 1.1.1 Analysis 1.1.2 Inspection 1.1.3 Simulation 1.1.4 Test Qualifying tests and other testing as mentioned below 1.2 Validation methods 1.3 Certification process 1.4 Acceptance test	2. Validation and verification of IoT Architecture End Result 2.1 Discrepancy reports 2.2 Verified product reports 2.3 Compliance documentation 3. Validation and verification Implementation 3.1 Verification and validation flow 3.2 Test parameters 3.3 Supporting Equipments 3.4 Facilities 3.5 Verification testing

Table 3.3: Individual Hardware Verification Parameters with Tentative Plan

Step No.	**Parameter for verification**	**Software Verification tentative plan with Analysis, Simulation, demonstrations, inspections and other test**
1.	**Input**	1. Processes testing of individual module 2. Connect processes in sequence from one to N, and test after each new process addition 3. Test for making changes easily for processes 4. Component testing 5. Test for making changes easily for components Connect components in sequence from one to N, and test after each new component addition 6. Package testing 7. Test for making changes easily for packages 8. Connect packages in sequence from one to N, and test after each new package addition 9. Complete software system testing
2.	**Output**	
3	**On hardware /Instruments**	
4	**Time Complexity of a code**	
5	**Time For Retrieval**	
6	**Space Complexity of a code**	
7	**Memory For Results**	
8	**Security measure taken in a code**	
9	**Scalability of a code**	
10	**Power Consumption because of code execution**	
11	**Filtering of data of a code**	
12	**Self management/ Intelligence**	
13	**Semantic HI of Data of a code**	
14	**Portability of Code**	
15	**Legacy software compatibility**	
16	**Test for every possible application functioning**	

Table 3.4: Software Verification Parameters with Tentative Plan

Step No.	Parameter for verification	hardware Verification tentative plan with minimum software
1.	**Input**	1. Testing of individual Thing/Device 2. Testing of Thing and reader connected to each other. 3. Testing of number of Things / devices when connected together to form small local networks as per network technology, along with required additional hardware. 4. Testing of Various servers, data storage devices 5. Testing of an IoT network hardware (testing under all possible combinations)
2.	**Output**	
3	**Power Consumption**	
	QoS of network	
	Life of individual device/ Thing, or other infrastructure	
4	**Self management/ Intelligence**	
5	**Security**	
6	**Scalability**	
7	**Portability**	
8	**Temperature, pressure, vibrations testing**	
9	**Location testing i.e. space, under water, under normal conditions etc.**	
10	**User friendly/ ease of operation**	

Table 3.5: Complete System Architecture Verification Parameters with Tentative Plan

Step No.	Parameter for verification	Complete system Verification tentative plan with minimum software and hardware
1.	**Input**	1. Individual Thing/Device test with software modules or packages execution 2. Testing of Thing connected to reader device with software modules, packages. 3. Testing of number of Things / devices when connected together to form a small local networks as per network technology and software, along with required additional hardware infrastructure 4. Testing of an IoT network (testing under all possible combinations, use of networks etc.) with software modules, packages
2.	**Output**	
3	**Simultaneous working of random number of users (in thousands, millions, etc.)**	
3	**Power Consumption per day**	
4	**QoS of network**	
5	**QoS of application**	
6	**life**	
7	**Self management/ Intelligence**	
8	**Security s/w, h/w, human, atmospheric etc.**	
9	**Scalability**	
10	**Portability**	
11	**Temperature, pressure, vibrations testing**	
12	**Location testing i.e. space, under water, under normal conditions etc.**	
13	**User acceptance test**	
15	**Simultaneous retrieval and storage**	
16	**Time for finding service**	
17	**Time for retrieval of information**	
18	**Services offered**	
19	**Plug and play feature of hardware**	
20	**Mobility of Things and its connectivity**	
21	**Cost**	

Table 3.6: System Validation Plan

Step No.	Parameter for Validation	
1	Real / Simulation environment	Validation of Complete IoT system architecture
2	Customer, sponsored acceptance test	

Verification will confirm the correctness of theoretical design of IoT architecture. Validation will further add whether, the design is really working for the required application. As per results of test for both, corrections can be made and final IoT architecture shall be available.

3.5.2 Abstract IoT Model validation with Arduino

It is one of the tool [139] wielded for experimentation of IoT. Proposed abstract IoT model of architecture is validated. The scenario considered is light intensity monitoring through internet. Efforts are made to build architecture as generic. Generalization is implemented in reading and saving the resistance values because of Light intensity values. Whenever application wants to read save and display the value, this architecture will be useful. As processing and output requirements of various applications are different, it is not possible to build these components as generic in this application.

Figure 3.10 displays the block diagram for remote light intensity monitoring system. Circuit assembly requires Arduino - UNO board, Ethernet shield, Light dependent resister, 4 port ADSL modem router, and RJ 45 cable. The Ethernet Shield connects Arduino to Internet. Specifications of Ethernet Shield are as follows

1. Processor ATmega328 microcontroller
2. Operating voltage 5V (supplied from the Arduino Board)
3. Ethernet Controller: W5100 with internal 16K buffer
4. Connection speed: 10/100Mb

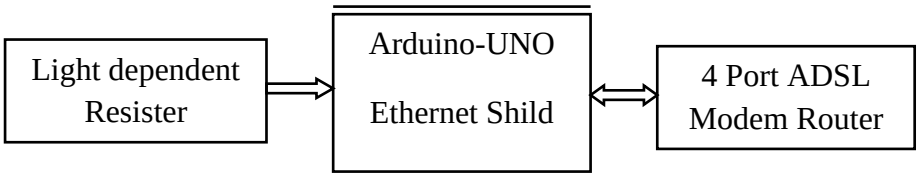


Fig. 3.10 Remote LDR monitoring system

Arduino IDE is required to be installed along with SD card, Ethernet and other basic libraries on the PC/ Laptop. Connect the shield to Arduino board, LDR to analog port 0 and two RJ45 cable from router to PC and Arduino board respectively. Power on Arduino by connecting

power cord to USB of PC. Insert SD card into the slot provided on shield. Upload program monitor execution serially. Sketch is as follows.

1. Check if you get router IP address and display messages accordingly.
2. Upon successful reception of IP from router, provide Mac and IP address of Arduino assembly and upload sketch to Arduino. Check if it is printing respective IP addresses or not.
3. Connect LDR to analog port 1.
4. Upload sketch for monitoring the data on Internet, and save reading in SD card.

Step wise results are displayed in figure 3.11a to 3.11f.

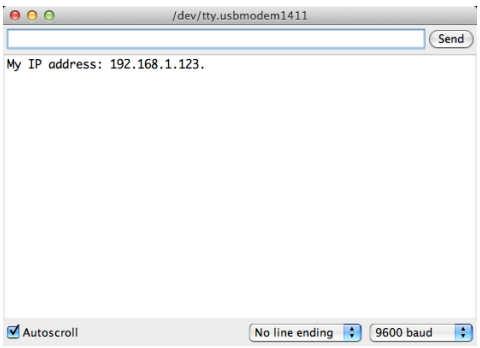


Fig 3.11a: Checking router address

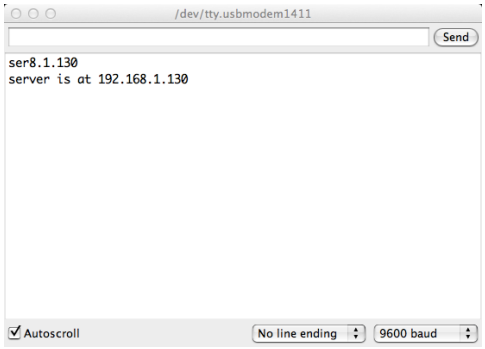


Fig 3.11b: Shield IP address

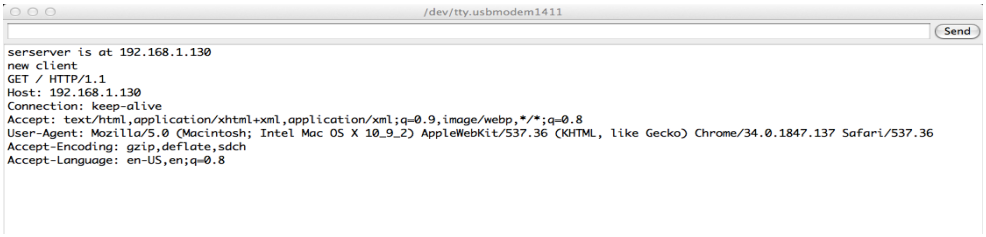


Fig 3.11c: Accessing shield as a client Figure 3.11a to 3.11c confirms working of shield as a server and PC as a client, after uploading the sketch in Arduino.

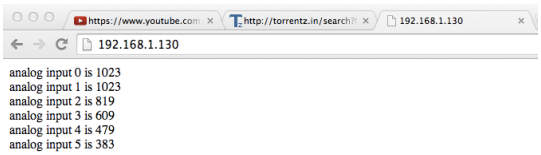


Fig 3.11d: Temp. before monitoring

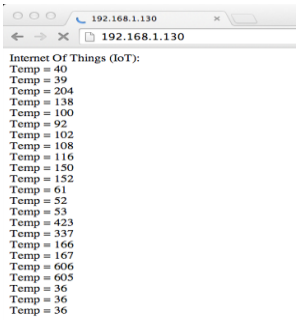


Fig 3.11e: Temp. after monitoring

Figure 3.11d checks that total 5 analog ports are used here for testing and shows garbage value as nothing is connected to all these ports (Individual pins are called as ports). Figure 3.11e shows the readings of resistances because of LDR. It is connected to port one (analog

port one). There are various values of resistors. Range of 30 to 40 represents value as zero (LDS if exposed to high intensity light). Increase in the resistor range represents shift of light from higher light intensity to lower intensity. Readings are sent to client by server at the set interval (delay function) e.g. can be 1ms, 2ms etc.

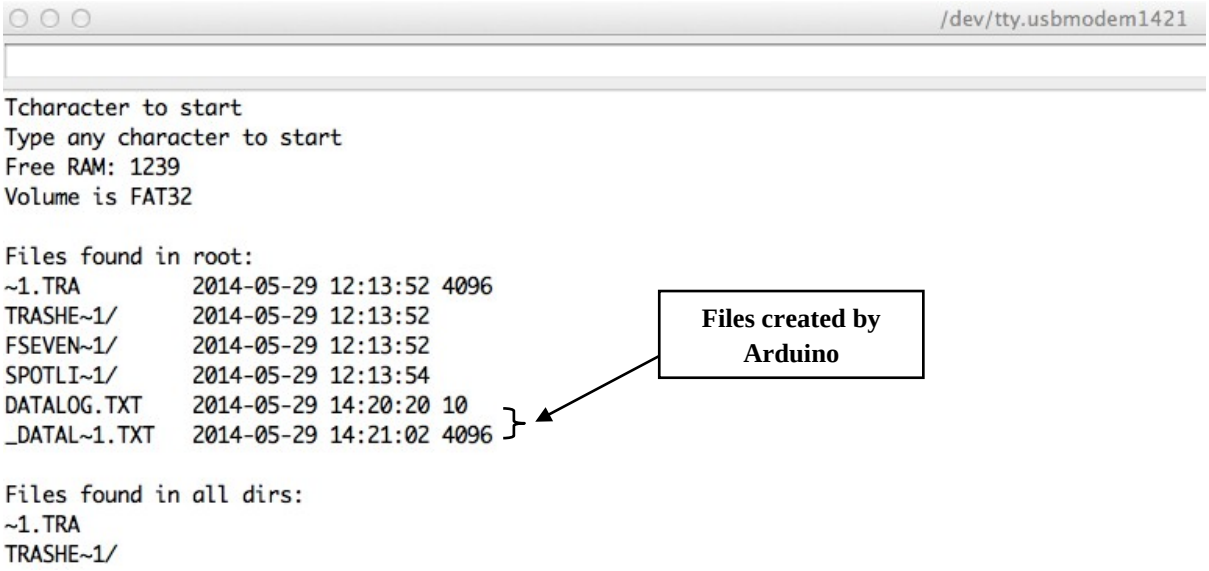


Fig 3.11f: data logged in new created file datalog.txt or datalog1.txt

Arduino provides facility to store readings of a sensor in SD (secure disk) cards, and known as data logging. Micro SD acts as a storage device. File named datalog.txt is created by Arduino and stores sensor readings. Figure 3.11f shows files created as datalog.txt or datalog1.txt. This feature can be said as one of the aspects, in generic IoT architecture design. Experiment results prove the working of proposed abstract IoT model. It can be said that we have validated the IoT application.

3.6. Proposed scalable IoT Architecture Model

Scalability [137-38] is the ability of system architecture, individual, any network, or all networks, or processes of communication to handle a growing amount of functions related with it, while maintaining quality. Scalability can be achieved with the hardware and software combination. Scalability can be measured in various dimensions like administrative, functional, geographic, and load scalability. Scalability performance can be in increasing or decreasing order of interest. E.g. bandwidth utilization shall be increased or transmission delays shall be decreased. At each and every place, it is expected that the scalability feature is available. E.g. process, component, module, network. But to get scalability, care has to be taken into the architecture design of any application.

3.6.1. IoT scalability

For designing any architecture, it is necessary to finalize the methods in an application. The finalized methods decide infrastructure, network type, security concerns, and all the other architecture related requirements.

Two main methodologies are TCP/IP and range increment of constrained node for IoT are important from scalability point of view. Connecting constrained things to the Internet was a major step for the enablement of IoT. The invention is done for constrained devices for 8 or 16 bit controllers. This invention scales down the TCP / IP protocol from unconstrained devices to constrained devices. Minimum features in TCP /IP are implemented from providing the Internet connectivity point of view. This is a decreasing required scalability.

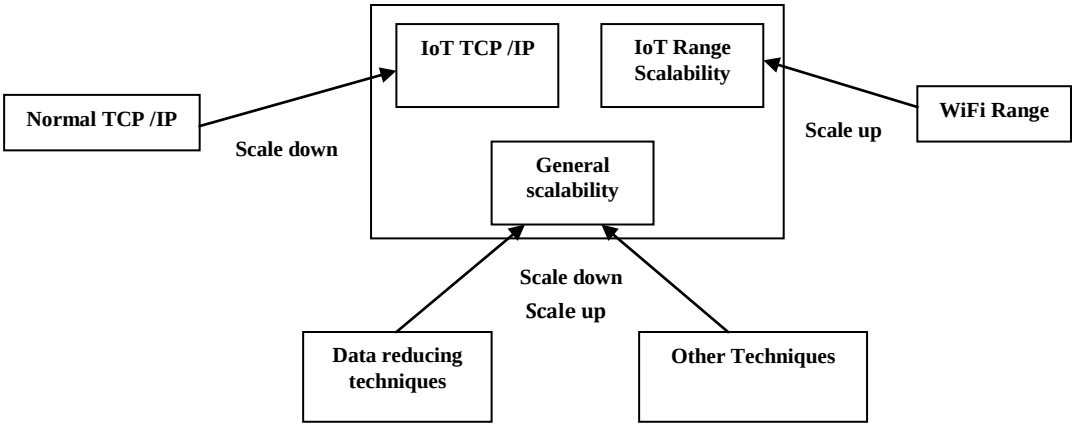


Fig 3-12: IoT Architecture Scalability model

The next major step required is the connectivity of IoT devices to Wi-Fi. It can be done by increasing the power of devices indirectly for increasing the range. It is difficult to place a number of gateways for such small peripheral networks. Or else by any other means connect these devices to the Wi-Fi access point. This can be thought as an increasing scalability.

Range enhancement is required to be worked further. General scalability may lead to any features like power consumption, data volumes, interoperability, service discovery, device discovery, etc. Refer to figure 3-12 for IoT scalability model.

3.6.2 The Proposed solution for scalable IoT architecture using data reduction techniques – by encoding data at the source level.

Information is sent continuously from Things to the server. This Information will be fixed for a specific application. E.g. ambient. A proposed method will lead to care taken at the root level logic, which will turn into a large achievement of scalability of time of transmission, storage, and power consumption at a complete IoT network level and at node level also. Data

reduction scalability will be useful for reducing the processing time, reducing data transmission time, reducing traffic, reducing power consumption, and reducing the data storage requirements. When a node is moving from one network to another network data has to be converted from one protocol packet format to another protocol. If this data is small in size, all processes in conversion will be reduced.

Information read from things can have a number of bytes in it. These values (readings) will be sent number of times as per requirement of application e.g. every hour, day, when reading goes above or below safe range etc. We can partition all the readings of an application as per its sensitivity and accuracy requirements. E.g. an allowable reading range at both ends (lower and upper), problematic reading range, or a severe problem range and so on. Almost all sensor Things applications will have a fixed range of values, which are required to be transmitted repeatedly.

Sensor (Things) reads the physical parameter and then is converted to digital one with the help of ADC. Then, from ADC it is taken into the microcontroller to send it to the required output device (e.g. LCD, LED etc). For example, here, if the reading is 3.35V, the microcontroller logic jumps to find out the equivalent ASCII value for 3, dot**,** and five. Totally, it jumps four times to the ROM memory to find the required ASCII values. These values are then sent through wireless communication for Internet services.

Here, we suggest that, in the ROM one character of 1B shall be stored for each defined range instead of four in above example. These characters shall be sent for the respective readings, and then shall be decoded as per the characters sent by the receiving end. This is going to help in power consumption of the extra three jump operations in the above example (3* number of readings sent in a day). Also, the ROM requirement will be reduced from 256 characters to hardly 10 characters (assuming we have assigned various characters for these ranges). As the numbers of bytes sent are reduced, further all the processes in transmission are reduced.

Simple simulation can help to prove the logic. We can simulate with the first one byte transmission and then two bytes. A reading can be taken for encoding of one, two three etc. bytes as well as for power consumption for one, two three bytes transmission. Reduced data means less intermediate processes. This results in a huge vertical scalability of power consumption of an individual node, and Internetwork. Traffic is reduced resulting in avoidance of a collision. The characters set for ranges can be different for various applications, and this will improve security.

3.7 IoT Applications

The IoT application list is very huge or can say as unlimited. Individual IoT applications to country level applications are enlisted here. The IoT helps in monitoring and controlling various tasks of individuals, cities, and countries to be done automatically. from anyplace and at any time. Users can be individual, societies or governments. The object for which, such applications are executed is said to be smart. E.g. smart thing, smart city to smart country. The IoT can be extended further for smart universe. It is not possible to mention each and every application, so few are mentioned. Survey papers covered in chapter two lists almost all applications.

Personnel (Human) - health monitoring like blood pressure, diabetes, heart attacks, pathology reports, etc. and sending to respective doctors. Monitoring and controlling eating habits.

Smart homes – temperature, fire, theft, electricity meter, water meter, Gas leakage, smart freeze, smart grocery rack, smart food rack, monitoring people coming into the house, smart TV, monitoring house construction condition, monitoring atmospheric changes in house other than above, monitoring and controlling all bill payments , tax payments and bank transactions.

Smart Cities

- Government tasks- monitoring and controlling street light, water (provide facilities as per availability etc), bills by citizens, checking conditions of water, roads etc. various taxes monitoring and controlling (if not paid by individual send message or block account etc. actions can be taken). Smart parking, smart local transportation and other transportation means (trains, aeroplanes etc), smart hospitals, smart building, and many other tasks...
- Industrial – automobiles, communication etc...

Smart country – defence (monitoring, controlling and protecting borders of a country), Environmental, agriculture, energy consumption by natural resources, and many more.....

3.8 Conclusions

Software architecture – Requirement analysis, static and dynamic modelling frames an overall idea of IoT software architecture and the hardware on which, it is executed. UML modelling has a limitation of expressing dynamic processes as per event generation. The dynamic process is at a very abstract level. Individual software components can be further modelled with class diagrams using UML. Activity and dynamic modelling requires a sensor modelling language. Software and concrete system reference architecture is not seen in any papers or research.

Abstract Generic IoT System Reference Architecture - It is a combination of software and system architecture. Perspectives covered cannot be reduced or omitted. Architecture design does not consider gateways as adaptable protocols are expected. Architecture is applicable for logical as well as for physical locations of Things. All points are covered to make IoT architecture as generic. Virtual Things are not considered as itself it is a very huge domain, but the proposed architecture is applicable for it also.

Scalability in architecture –Horizontal and vertical scalability can be achieved by increasing hardware and node's resources. But it is expected that these hardware and resources shall be utilized in a very efficient and optimized way, so as to improve the vertical scalability. Reduction in data at source will result in large vertical and horizontal scalability of all processes in communication. Thesis has proposed one method for it.

In general, conclusion can be drawn that Abstract Generic IoT System Reference Architecture is proposed theoretically. One of the non functional feature scalability of architecture is proposed theoretically and proved practically. Monitoring light intensity as one of the IoT application following abstract IoT model as proposed is validated practically.

Chapter 4

Design of Heterogeneous Interoperable IoT Network architecture

4.1 Introduction

Chapter works on second non functional feature of IoT architecture as Heterogeneous Interoperability (HI) of networks. Things mobility of constrained devices in IoT requires gateways for translating information between two different networks, as it is not optimal to have number of interfaces on tiny constrained things. When a node moves from one network to other, handoff occurs. A seamless handover of data sessions is the main focus at the time of handover. Moreover, handoffs can be vertical or horizontal and can be network based or client based. Heterogeneous Interoperability of networks command vertical handover and so is a topic of our research.

TCP/IP protocol is scaled down [140] to 8 bit micro-controller in the form of uIP protocol. Next aim is to scale down OFDM technology for Bluetooth and Zigbee. Figure 4.1 displays simple outline of this chapter. Section one compares Wi-Fi, Zigbee, Bluetooth. State of the art of co-existence of Wi-Fi, Zigbee, Bluetooth, and all three or in pair is discussed in the same section. We propose new concept for heterogeneous interoperability of networks in section two. Section proposes the solution for vertical handoff (VHO) with co-existence of Wi-Fi, Zigbee, and Bluetooth. Wi-Fi access point is proposed with modifications and named as BZ- Fi. Name is entitled to indicate that all three technologies protocol stacks are present at one place. What is the need of co-existence of all three, challenges in it, all are discussed here. Section two also proposes the deployment of OFDM in Zigbee and Bluetooth technologies. Detailed discussion is provided with the challenges and possibility of implementation of OFDM in them.

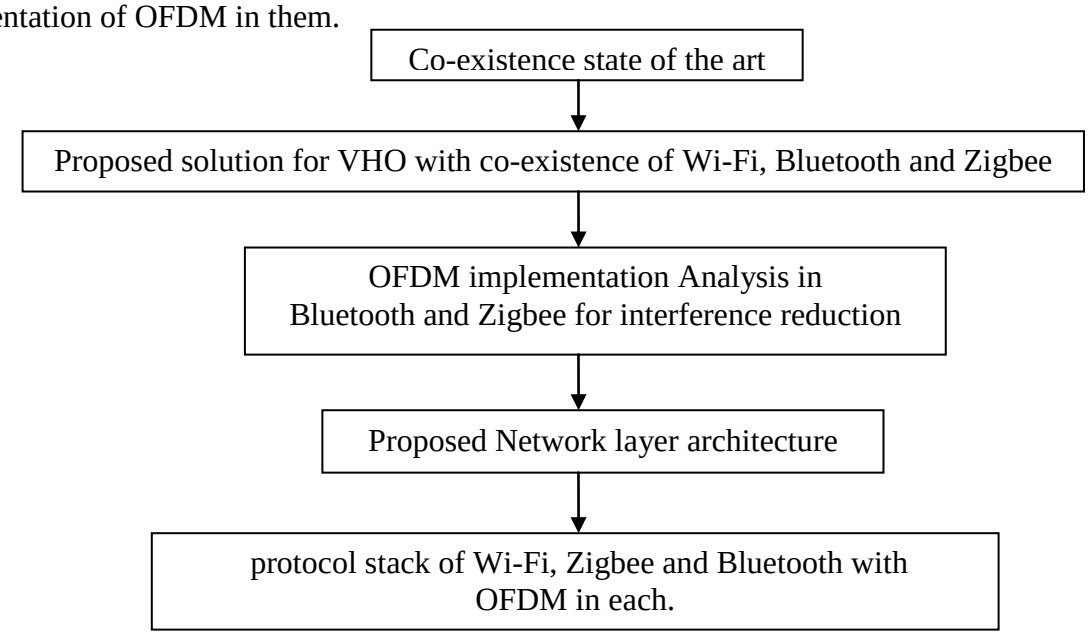


Figure 4.1: chapter flow diagram

Section three outlines the objectives of designing the heterogeneous interoperable network architecture i.e. for vertical handoff between Wi-Fi, Zigbee, Bluetooth networks. Network layered architecture for HI is proposed in section four. Network architecture implementation, participating node's functionality modules are specified layer wise for BZ-Fi access point and Bluetooth and Zigbee. Section also contributes the new protocol stack, with limitations of existing protocols for each layer protocol. Limitations shall be considered as service requirement of that layer in new protocol design. Chapter ends with conclusion section. Conclusions close the last section.

Complete sections two to five are contributed by author. Chapter is useful for improving the handoff delays, co-existence interference and will offers high speeds than existing.

4.1.1 Handoff Classification

Handoffs are classified into two main domains as Horizontal Handoff (HHO) and vertical Handoff (VHO) [141]. The distinction between them is denoted in the table 4-I.

Table 4-I: VHO and HHO Comparison

Parameters	VHO	HHO
Access Technology	Changes	Does not change
QoS Parameters	May be changed	May changed
IP Address	Changes	Changes
Network Interface	May be changed	Does not change
Network Connection	More than one connection	Single connection

Wi-Fi, Bluetooth and Zigbee all share ISM (Industrial, Scientific and Military) frequency band of 2.4 GHz. Comparison of three technologies is discussed in table 4-2.

Table 4-II: Comparison of Wi-Fi, Bluetooth and Zigbee [142]

Parameter	Bluetooth	Zigbee	Wi-Fi
IEEE specification	802.15.1	802.15.4	802.11
Range	10-100 m	10-100 m	50-100 m
Operating frequency	2.4 GHz	2.4 GHz world wide	2.4 and 5 GHz
No. of RF channels	79	1/10;16	14
Modulation type	GFSK	BPSK(+ASK), O-QPSK	BPSK,QPSK,COFDM
Co-existence mechanism	Adaptive freq. hopping	Dynamic freq. selection	Dynamic freq. selection
Security	16-bit CRC	16 bit CRC	32-bit CRC

4.1.2 Co-existence state of the art for Wi-Fi, Bluetooth, Zigbee

Most of the experimentation is done by researchers for checking the interference effect of all three technologies on one another or between any two pairs. Paper [143-44] says that Zigbee suffers a lot in co-existence of Wi-Fi than Bluetooth and effect of Wi-Fi on Bluetooth is negligible. Paper [145] deduces results for interference from co-existence of all pair combinations and effect on all three at a time. The same results are put up by Sikora and Groza [146]. IEEE 802.15.2 has discussed interference because of co-existence for Wi-Fi and Bluetooth. The co-existence of Wi-Fi with Bluetooth is already proved and implemented by Texas Instruments [147] and other researchers. Wi-Fi and Bluetooth co-existence on vehicular communication is studied in [148]. Wi-Fi and Zigbee co-existence was experimented [149-50] with dynamic frequency selection and transmission power control. Papers also provide issues of co-existence. Wi-Fi, Bluetooth and Zigbee co-existence scenarios are available for scattered constrained or unconstrained devices using these technologies and survey is available in paper [151]. From all above papers, it is concluded that co-existence of scattered scenario is still not solved completely. Overall study says that there is no solution available yet for co-existence of three at a single place or even at scattered place completely. Problems with co-existence are as follows

1. Zigbee standard don't support dynamic adaptation of frequency channel.
2. As IEEE 802.11b and 802.15.4 have same carrier frequency, impact of Wi-Fi on Zigbee is very critical.

4.1.2.1. Existing available solutions:

1. Out of three at a time any one is active, using multiplexer and demultiplexer at the access point, which makes any one technology active at a time. This technique is already in practice. Virtualization can be logic, which will be very much advantageous for providing services.

2. Various scheduling algorithms are applied to change the same carrier frequency.

3. Coding techniques can be also applied which can transmit the waves in required phase.

4. **802.15.4** May use free space between 802.11 two channels. Also channels 25 and 26 are available for Zigbee.

5. OFDM technique is available for interference removal, but not implemented in Bluetooth and Zigbee because of power constraints.

4.2 Proposed solution for Vertical Handoff between Wi-Fi, Bluetooth and Zigbee Networks (BZ-Fi)

Constrained devices have limited range of communication, battery power and computing power. It is very difficult to improve any of the foresaid factors. Constrained devices can't have number of interfaces. These three technologies share the same frequency band as 2.4GHz, but with different speed of data transmission, modulation technique and power. Wi-Fi access point has the highest features in terms of bandwidth, speed and power out of three.

4.2.1. Objectives of proposed logic

1. The main objective is to achieve heterogeneous network interoperability of constrained nodes.
2. To reduce number of interfaces on node, than its own technology for Zigbee and Bluetooth.
3. Zigbee and Bluetooth nodes will able to transmit and receive the information even if, they are in Wi-Fi area without gateway.
4. To eliminate intermediate time delays in handover and improve power consumption.
5. Increase the speed of transmission as a by product of OFDM implementation.

Block diagram 4-4 explains the expected logic. As per the packet format Wi-Fi, Bluetooth or Zigbee further processing block will take control.

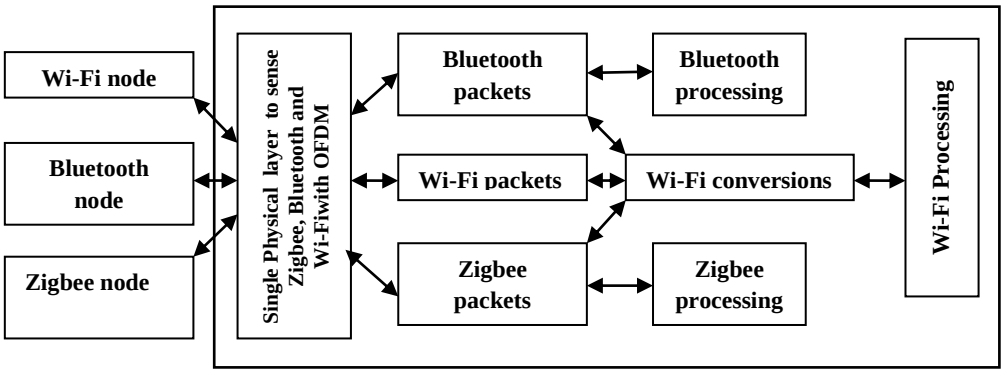


Fig4-2: Proposed BZ-Fi Access Point

If we want to convert all packets to Wi-Fi, then Wi-Fi processing blocks (acting as gateway) by default will function, else other blocks. In processing, speed, power and modulation techniques conversions are required. This modified access point is called as BZ-Fi. BZ-Fi working is explained below.

We expect that this proposed BZ-Fi access point will function like base stations. Consider the example of mobile base station and mobile device like cell phone. Phone has limited communication range and power as compared to the base station. But base station takes care

of transmission and reception of the packets to and from mobile devices. Here base station and mobile device both have same packet format, and frequency ranges compatibility. Wi-Fi lower limit is 50m as compared with 10m of Zigbee and Bluetooth. Higher power of Wi-Fi access point will help in increasing the ranges for Bluetooth and Zigbee, as Wi-Fi access point will sense these technologies out of range of these network areas. Access point should function in similar manner as base station, but with co-existence. Number of BZ-Fi access points will be there in a single base station cell. This network can be considered at the lower level than base stations and can be visualized in figure 4.3. There will be conversion from Zigbee / Bluetooth to Wi-Fi using dynamically reconfigurable protocol stack present in BZ-Fi. The target for data travel is Wi-Fi access point.

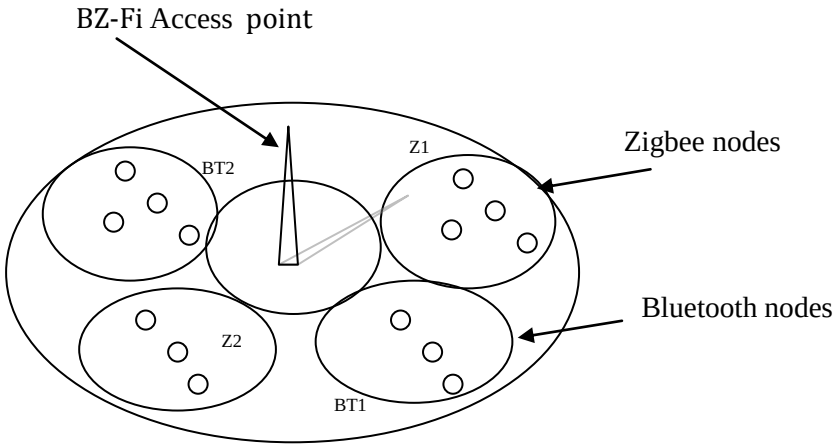


Figure 4.3: Co-existence requirement scenario with overlay networks

Figure 4.3 represents static scenario of BZ-Fi, Bluetooth and Zigbee networks. Few nodes may be moving as per need. BT1, BT2 and Z1, Z2 circles spots Bluetooth and Zigbee networks respectively. BZ-Fi access point shall sense any Bluetooth, Zigbee and /or Wi-Fi packets. BZ-Fi shall function simultaneously for Bluetooth, Zigbee and Wi-Fi. BZ-Fi internally, processes packets in the same technology as the incoming packet or as per the requirement. If node in BT1 wants to talk with node in BT2, it is not possible in normal conditions, as there is no Bluetooth node in between. But because of BZ-Fi, it can receive packets from BT1 and forward to node in BT2. This is nothing but increase in the ranges of Bluetooth and Zigbee. Bluetooth node may communicate with Zigbee node in BZ-Fi network.

Range increment in transmission and reception of data packets in Zigbee and Bluetooth is possible because of following reasons.

1. Wi-Fi has more power than Zigbee and Bluetooth.
2. Lower range limit of Wi-Fi is 50m as compared to 10m of Zigbee and Bluetooth.

Figure 4.3 signifies a single base station cell with multiple BZ-Fi cells, similar to base station cell arrangement. BZ-Fi cells shapes will be hexagonal in shape. Our focus at present is only on BZ-Fi. Present BZ-Fi will accept the data for Internet from Bluetooth or Zigbee primarily. Accordingly changes are required to be implemented in protocols. When node wants to send data to the BZ-Fi, accordingly request should be generated. Because of a single BZ-Fi cell, numbers of communication scenarios are possible between Wi-Fi, Bluetooth and Zigbee, which otherwise were not. Some of the scenarios are discussed below.

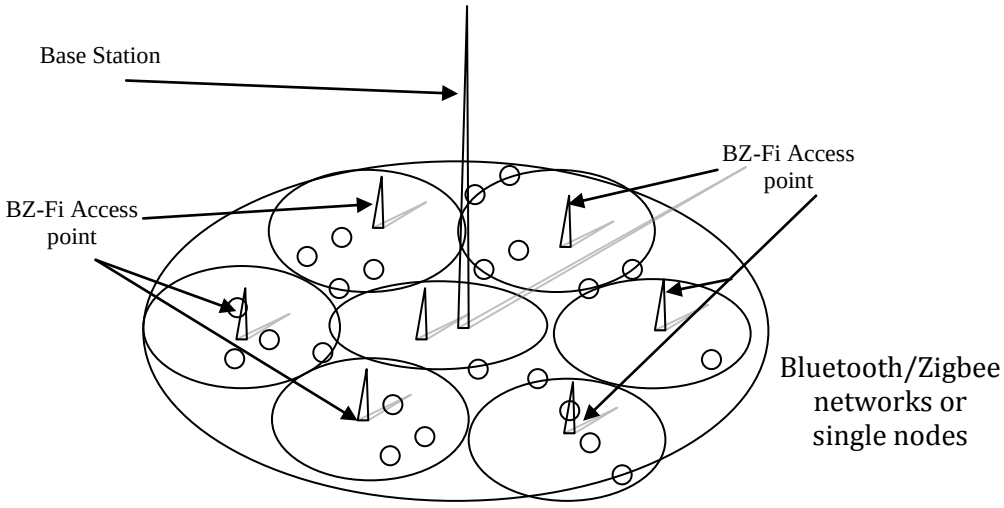


Figure 4.4: BZ-Fi access points cell network

Case 1 BT to BT communication in the same network- Bluetooth node is moving from its own network to Wi-Fi network (BT1 has moved to BZ-Fi while communication was in process with other node in the BT1). Node can be moving when call session is in process. In this case, Bluetooth node should be able to continue call session within the BZ-Fi network. Or if Bluetooth node wants to send information on Internet or want to talk to Bluetooth node of different network, same BZ-Fi access point will be useful. This is possible, only when either gateway (Wi-Fi to Bluetooth and vice versa) is present or Wi-Fi access point has Bluetooth interface.

Case 2 - Similar with above case instead of Bluetooth node, Zigbee node is moving into Wi-Fi with all above related conditions. Here gateways can be (Wi-Fi to Zigbee and vice versa)

Case 3 BT1 to BT2, BT1, BT2 to ZB, BT to Wi-Fi / ZB to ZB, ZB1,ZB2 to BT, ZB to Wi-Fi - It is an additional functionality. All communication possibilities of communication will be fulfilled (other than above) in these three network technologies. Zigbee and Bluetooth interfaces are present in the BZ-Fi access point. If Zigbee or Bluetooth nodes want to make a new call to other Zigbee or Bluetooth nodes outside their own networks, they can't. As these

nodes are outside the ranges of their own and other network nodes. So there is no alternative than to take a help of BZ-Fi access point for communication or gateway. BZ-Fi access point can send call request for other types of nodes in their own respective network technology format, and continue call sessions. At a time proposed access point should be able to connect to all three calls as Wi-Fi to Wi-Fi, Zigbee through Wi-Fi to Zigbee, Bluetooth through Wi-Fi to Bluetooth etc. Here two possibilities are present. First possibility is that, BZ-Fi access point acts as a gateway for these three heterogeneous technologies, when data is required to be sent to different technology node. Second possibility, data transmission is required in same format as received by access point. As per packet format (Zigbee or Bluetooth) next steps will be decided as represented in the figure 4.4.

There is an overlay of Zigbee, Bluetooth and Wi-Fi. Number of Zigbee, Bluetooth networks will be increased in future. It is concluded that to reduce handover time and reduce number of gateways for each of these networks, co-existence of three networks is required. If co-existence is there, interference comes into the picture. Sub section 4.2.2. provides solution

4.2.2 Proposed solution for interference reduction in co-existence of Wi-Fi, Bluetooth and Zigbee

Two solutions are proposed for interference reduction in co-existence of Wi-Fi, Bluetooth and Zigbee. They are as follows.

1. Zigbee is affected more in presence of Wi-Fi, so main focus is with Wi-Fi and Zigbee. OFDM is a very well known technology, deployed for inter symbol and inter channel interference removal with fast speed of data transmission. We propose the usage of OFDM technology in Bluetooth and Zigbee constrained nodes. Second advantage in embedding OFDM to Zigbee and Bluetooth, is increase in speed.
2. We also extend further additionally and propose to transmit and receive Wi-Fi and Zigbee OFDM waves orthogonal to each other [152] or perpendicular to each other, Along with OFDM, we suggest transmitting Zigbee (Bluetooth) waves orthogonal to Wi-Fi, Which can be a second effort in avoiding collisions. Sending Zigbee in perpendicular manner with Antenna polarization, number of collision may reduce further to some extent. All Zigbee nodes by default should transmit and receive waves in a perpendicular manner to Wi-Fi permanently. Bluetooth will continue its normal TX and RX using OFDM. Antenna polarization can be done externally.

4.2.3. Analysis of OFDM implementation in Bluetooth and Zigbee

The Bluetooth system employs a frequency hop transceiver to combat interference and fading, and provides many FHSS carriers [153]. Frequency modulation reduces transceiver complexity. The basic hopping pattern, excludes the portion of interfering frequencies. It also improves co-existence with static (non-hopping) ISM systems.

The Zigbee system employs direct sequence spread spectrum (DSSS) to eliminate [150] co-existence problem. We can see that major reasons for using FHK and DSSS in Bluetooth and Zigbee respectively is to eliminate co-existence and making transreceiver light. Power consumption and memory are two parameters, which have to be checked for OFDM in these technologies.

The frequency band, Channels and data speed for three are mentioned in figure 4.II. We analyze further probable features required for OFDM implementation in Zigbee and Bluetooth. Here simple mapping of some of the requirements is analyzed.

1. **Power consumption**

   OFDM is a combination of lots of functionalities. The most computationally complex function of OFDM modulation is IFFT and FFT. The major issue is power consumption by these blocks. If it is implemented with ASIC, power consumption, and area can be reduced drastically as compared to DSP processor. Paper [154] works on power consumption issue of FFT using fabric, Xilinx FFT core, and non reconfigurable ASIC. The results confirm that very less power (less than 10mW) is consumed for small FFT size (up to 64) for fabric, and ASIC. For FFT size up to 1024 the power consumed is between 68 to 82 mW. Area required for implementation in fabric is 2.86mm^3 (for all FFT size 16 to 1024), and .07 to 2.51 mm^3 (for FFT size 16-1024) for non reconfigurable ASIC. Similarly IFFT will also have near about same power consumption.

   Paper [155] experiment, with the CNEM FPGA architecture achieves an average 98%, 85%, 71%, and 99.99% reduction in critical path delay, routing energy, total energy, leakage power over CMOS (180nm) FPGA architecture. This CNEM FPGA architecture can be tried for reducing power consumption in IFFT and FFT.

   The research is going on for ultra low power devices [156]. If this research becomes successful, then above power requirements will be reduced by 90-98%. This will further reduce the power consumption drastically, making implementation of OFDM in Zigbee and Bluetooth very easy.

Analysis can be summarized with example, that if node consumes 10mw, with the implementation of CNEM, it will be reduced to 3mw or even to .2mw with ultra low power inventions.

There can be problem when the node consumes very low power (e.g. 1mw etc.) In that case OFDM implementation may not be possible. But otherwise there should not be a problem in implementation. Above discussion helps proposed logic, of OFDM implementation in Bluetooth and Zigbee from power perspectives. Bluetooth has power consumption 100mW and Zigbee has 30mW. For Bluetooth we can **take efforts for** FFT and IFFT size from 16 to 256. And for Zigbee we can **go** up to 256 FFT and IFFT size.

2. Memory

Addition of OFDM [157] will require DSP processor or FPGA (field processing gate array) alternatives and whole OFDM transreceiver shall fit in the memory requirements of KB. OFDM implementation requires more memory for IFFT and FFT. Memory can be reduced if radix method is worked for FFT and IFFT implementation. Table 4.III compares memory requirements with and without radix methods.

Table 4.III: Memory calculations for FFT and IFFT

No. of point N	Direct computation			FFT computation					
	Complex addition N^2	Complex mul. N^2-N	Total memory required Bits	Radix 2= 2^V v=1, 2, 3…..			Radix 4= 4^V v=1, 2, 3…		
				Complex addition $N\log_2 N$	Complex mul. $N/2 \log_2 N$	Total mem. reqd 2N+N/2 Bits	Complex addition $N\log_2 N$	Complex mul. N/2 $\log_2 N$	Total mem. reqd 2N+N/2 Bits
4	16	12	28	4	8	12	-	-	-
8	64	56	120	12	24	36	-	-	-
16	256	240	496	32	64	96	32	64	96
32	1024	992	2016	40	80	120	40	80	120

Here, the number of points N represents samples. Direct computation method caters the memory required for complex addition and multiplication using discrete Fourier transform. In case of direct computation complex addition requires N^2 memory space and complex multiplication requires N^2-N memory space. In case of FFT computation we are using radix2, radix4 methods for complex addition and multiplication. In case of radix 2 method we can calculate in terms of power of two i.e. 2^n. In case of radix4 method we can calculate in terms of power of 4 i.e. 4^n FFT processes calculation faster as compared to the direct computation method. So, the memory space required is also less for FFT manipulation.

The total memory locations can be calculated by 2N+N/2 in case of FFT. Radix2 method can calculate up to $2^{n.}$ So for fast manipulating, we prefer the radix 4 method when the no. of input samples are more. Also, we can manipulate the large no. of FFT together with the help of split radix form by combining radix2, radix4. We can construct the radix8, radix10, etc. as per the requirement. In case of FFT computation complex addition requires $N\log_2 N$ memory locations and complex multiplication requires $N/2 \log_2 N$ memory locations. Total memory required can be calculated by 2N+N/2.

Zigbee has flash memory between 60 KB and 256 KB, few KB of RAM and Bluetooth has 8-16M bit flash (in KB) and internal RAM in 250 KB. From the table 4.IV, we can conclude that radix method requires less memory and can be worked for available memory of Zigbee and Bluetooth. We summarize that, memory shall not be a constraint for OFDM implementation in Zigbee or Bluetooth.

3. Standardization problem

Next challenges are to implement the OFDM requirements in the Zigbee (and Bluetooth) physical and MAC layer frame formats i.e. TX and RX designs. As modulation is changed physical and MAC layers of Zigbee and Bluetooth will be changed. We can try same frame formats [158] as the existing once for Zigbee and Bluetooth (only frame format shall be same, but other physical and MAC layer functionalities will change as OFDM modulation). We try to examine the physical layer mapping below for Zigbee [159]. On the same line efforts are required to be carried out for Bluetooth. There are lots of differences in the physical layer frame format of 802.11g OFDM and Zigbee. In the transreceiver design, we assume that some of the parameters will be taken as default and will be known to every transreceiver. These parameters are implemented in hardware and software directly, instead of sending before every communication. This can be helpful in omitting some of the fields or reducing some of the bits in the frame fields. E.g. speed, modulation type etc.

3.1.1. Preambles

3.1.1.1. SYNC field-Both preambles have two common fields as synchronous and Start Frame Delimiter (SFD), but the number of bits are different. SYNC field is 56 bit for OFDM, where as it is 32 bits in Zigbee. A receiver starts synchronization after detecting SYNC. An 802.11a routine performs packet detection routine in 2/3 rd time of short preamble time slots [160]. We can make a try here with 32 bit synchronization bits with lower number of sample of symbols. Paper [161] has the synchronization process of OFDM transmitter and receiver with only two special symbols. Symbols are operated with the wobbulation and the Barker code. We can try in the same way for above two methods. This reduces sync field length.

3.1.1.2. SFD Field - SFD is spescified common for all IEEE 802.11 DSSS radios and holds fixed hexadecimal word as F3A0hex. 1B present in Zigbee should be checked further if sufficient in Zigbee. It is 2B in OFDM 802.11g and 1B in Zigbee.

3.1.2. PLCP header

3.1.2.1. PHY header – it has fields related with rate, length and fields for Burst modes of data transfer. We assume that in Zigbee, there is no need of burst mode. So all fields related with it can be omitted.

3.1.2.2. Signal field- Function of this field is to identify the type of modulation that the receiver must demodulate the signal. Zigbee employs DSSS modulation technique as a practice, so we can set it as default, in all Zigbee devices, to eliminate the field.

3.1.2.3. Service field- In 802.11g most of the bits are reserved for future. Bit 3 is meant for extended data rates. This bit concept will not be applicable as such for Zigbee (We assume here one fixed data rate will be worked). So this field can be omitted and will support for Zigbee fame fields.

3.1.2.4. Length field- It indicates the information MAC is expecting from PHY to transmit as compared with 12 bits in 802.11, here we have 7bits. This has to be worked further.

3.1.2.5 MAC Header- MAC accepts MSDU from higher layers and adds headers and trailers to create MAC header. Some fields are meant for supporting network connectivity of mobile nodes. In the Initial stage, we think of Stationary nodes only, eliminating the extra fields. Also we assume that communication is one to one and multicasting type. This will also eliminate some bits in address fields of 802.11 frames. And then remaining fields, match with the MAC header of Zigbee.

3.1.3. PSDU- variable length Data with OFDM modulation is sent. The PSDU frame format for Zigbee is 48bits (header) + PSDU<=127Bytes.The PSDU frame format for Bluetooth is Access code (72) bits + header 54 bits + 0-2754bits payload. The PSDU frame format for OFDM is 40bits (header) + variable DATA of OFDM. Above frame formats state that, sufficient bits are present in Zigbee and Bluetooth to follow OFDM frame logic.

MAC layer and physical layer protocols for OFDM will vary in both Zigbee and Bluetooth. IF physical layer is changed because of OFDM, considering the advantages of speed and less interference, new versions of Zigbee and Bluetooth standards will come into picture. More detailed **study** is required for the mapping of each and every functional requirement of the OFDM in the Zigbee and the Bluetooth. Accordingly, it may be required to optimize some blocks, or reuse some blocks in the multiplexed manner. Scaling of the OFDM to Zigbee and Bluetooth is required to be done.

Above analysis deduces that OFDM implementation can be tried in Bluetooth and Zigbee even with power, memory and other constraints. At present implementation of the IoT applications has just started. In future, number of devices using ISM band, may increase drastically leading to interference. Increase of speed of data transmission, with co-existence feature with Bluetooth and Zigbee, will be highly appreciated and accepted.

3.1.4. Challenges of proposed solution

It is understood that new TX –TX designs are required to be implemented. While practical experimentation all above changes one by one shall be carried out.

1. Biggest well known challenge is the channel interference for 2.4 GHz frequency band for three technologies at a single point or scattered one.
2. Traffic is required to be managed as all packets will be diverted to access point.
3. Scaling down of OFDM successfully in Bluetooth and Zigbee on power, memory.
4. From Standards perspectives- the implementation may result, the Zigbee and Bluetooth standards intact, else how much proposed solution is required in practice, based on its importance will lead to new standard.
5. As per above suggestions complete transreceiver of Bluetooth and Zigbee with OFDM have to be implemented, tested and then accordingly reformed.

4.3 Design goals for constrained node and BZ-Fi AP Heterogeneous interoperable Network architecture

Architecture should achieve the following goals

Communication network can be as overlay or neighbour independent networks of Wi-Fi, Bluetooth and Zigbee. The proposed logic will try to overcome the co-existence challenge in three networks with implementation of OFDM in Bluetooth and Zigbee and BZ-Fi increases the communication range of Zigbee and Bluetooth. Wi-Fi access point is assumed to have the communication with Bluetooth and Zigbee having various speeds and power. The network architecture at the constrained node side will be according to Bluetooth or Zigbee protocol stack with modifications in MAC and physical layers for OFDM implementation. Requirements are mentioned to eliminate the need of various interfaces (i.e. for Zigbee, Bluetooth) at constrained node, as a problem of main focus along with internet connectivity and other functions of each stack .The network architecture layers for Wi-Fi, Bluetooth or Zigbee are explained.

Points one to four are proposed changes, in the network architecture. Other points are stated as in general requirement of any constrained node and out of scope of our objective.

1. Nodes with Bluetooth interface shall be able to communicate with Wi-Fi interface nodes with the help of proposed new Wi-Fi Access point without gateways, like horizontal handoff. Here scenario will be a Bluetooth node communicating with Wi-Fi access point (using OFDM) and vice versa.
2. Zigbee node, RF wave should be transmitted or received perpendicular to Wi-Fi radio, at all the time. As a rule, the logic should be applied everywhere. Polarization of antenna can be considered further for co-ordination between physical layers.
3. Wi-Fi access point node will have three interfaces as Zigbee, Bluetooth (already available) and Wi-Fi itself, for co-existence of all three technologies. Bluetooth and Zigbee stack should be added into Wi-Fi AP stack. Bluetooth stack support is already available in Wi-Fi.
4. Routing layer should support the decision of horizontal handoff (as vertical hand off works as horizontal because of proposed logic), for actual physical routing for Bluetooth and Zigbee.

5. Functionalities should be available for virtual routing in Wi-Fi access point. Virtualization at Wi-Fi access point after co-existence can be useful to provide services and achieve vertical and horizontal scalability.
6. Nodes should be able to connect to the internet even with any constrained devices.
7. Support for standard and non standard things connectivity at the physical layer along with plug and play provision is required.
8. Packet sizes, header sizes and frames shall be handled as per the node computing power. The network should manage it with compression, fragmentation, reassemble or other logics required.
9. Support for security of static as well as dynamic, scalable topologies is required. As things can be moving, network control and maintenance is at end level, with expected self awareness capability.
10. As topology is dynamic or scalable, centralized monitoring is not possible. No centralized monitoring will be there.
11. Architecture should support generation of simple, uniform data format understandable by any application. It should filter data where ever possible. As per value of data, triggers/ events should be generated for required action at MAC layer.
12. It should connect itself to the core network using existing infrastructure without much change.

Guideline for design of any network architecture by analyzing communication mechanism and user interfaces is discussed in [162-63]. Constrained node is a peripheral node and can have basic layer architecture [164] with modifications in it as proposed. In our case we consider the case of communication between Zigbee / Bluetooth to Wi-Fi and vice versa. Network architecture for this scenario is a specification of layered hierarchy, and modules on the layers of nodes which perform defined functions. Network architecture specifies the functions of these modules, relationships between them, interfaces between same layers of different nodes and protocol stack for same layer communication. Modules in a layer hire services offered by lower layer.

4.4 Proposed Bluetooth or Zigbee nodes Heterogeneous Interoperable Layer network Architecture

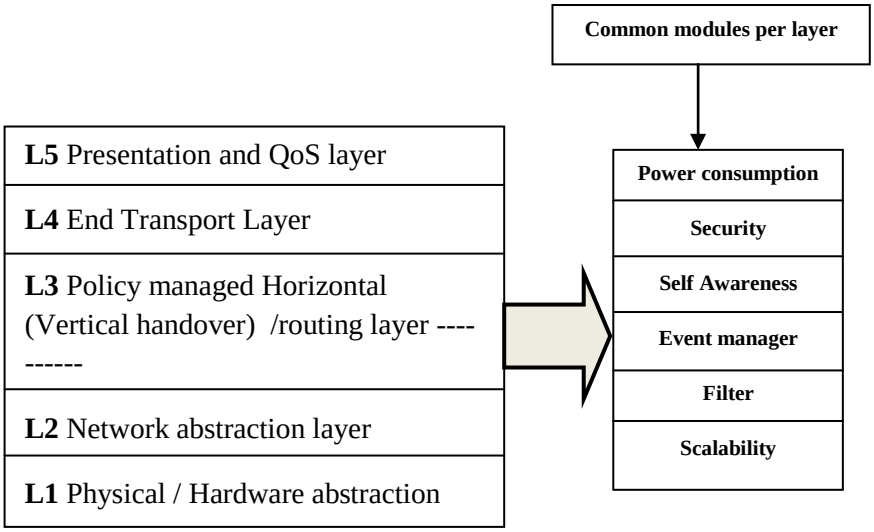


Fig 4-5: Proposed HI Network architecture layers for Zigbee or Bluetooth nodes

1. Proposed architecture (fig- 4-5) is five layers, peripheral network architecture for vertical (same as horizontal in our case) handoff. All five layers will do their own jobs, along with taking care of security, power consumption, self awareness, event manager, filter and scalability. The layer services are as follows. Modules present at different layers of constrained node (Zigbee or Bluetooth) are as indicated in the figure 4.6 and protocol stack is displayed in figure 4-8 respectively for constrained nodes. Figure 4.7 presents modules at different layers of BZ-Fi access point.

4.4.1 Layers

1. **Layer 1**- Physical / hardware abstraction/ - This layer will have major changes in the transreceiver because of OFDM. Totally new design is required. It will have channel coding and decoding, symbol mapping and de mapping, serial to parallel and vice versa blocks, IFFT and FFT, cyclic extension, removal of cyclic extension, DAC, ADC , TX and RX blocks. It shall also send Zigbee RF perpendicular to Wi-Fi RF (or vice versa) as Zigbee is affected more by Wi-Fi. Constrained node will have provision for perpendicular RF reception and transmission. In BZ-Fi access point, perpendicular Zigbee RF sensing feature should be made available. Layer should support OFDM packet frames.
2. **Layer 2**- Network abstraction layer /Data link layer - This layer will also undergo major changes for supporting OFDM transreceiver. Node is expected to transmit and receive

wireless packets in Zigbee / Bluetooth OFDM format in Wi-Fi range also. The layer should implement OFDM modulation technique at MAC layer of Zigbee or Bluetooth. The layer should support configuration, authentication, security, QoS, power control and transmission scheduling. Zigbee / Bluetooth and Wi-Fi network interfaces shall be used to maintain and control the network connectivity of the mobile things.

At BZ-Fi node MAC layer should support the Zigbee and Bluetooth functions. OFDM Modulation controlling functions would be there in Zigbee and Bluetooth.

3. **Layer 3** – Network Layer – Layer performs policy decision for physical routing functions mainly. Here it is possible that Wi-Fi access point is acting as an intermediate node for destination. Two modes of routing are required. First routing is from constrained node to Wi-Fi or vice versa. Second routing style is between nodes of same type with normal hopping method for communication. Destination node will be found out as per policy decisions for vertical handoff through Wi-Fi AP. Once the policy is fixed, locating a destination node physically will be carried out.

   Policy managed vertical or horizontal handover layer [7-8] or routing layer takes decision on various parameters like signal strength, bandwidth, service type and QoS, Cost, network, security, power consumption, mobility pattern, and MH priority. This layer will decide the policy logic for it. Layer is responsible for routing of data from one network to another network.

   Network's parts can be virtualized for efficient utilization of resources. Information of these virtualized networks shall be applied at the time of routing. This functionality will be for Wi-Fi access point. Node, wireless and wired links, processes, location time and other resources can be virtualized. Routing layer will select such path towards destination node. When these components are again internally isolated, selection of those specific out of many is again required for completion of routing. This is a responsibility of virtual routing layer. It will select a specific path out of many virtualized, time and location slots out of many, Node's other resources. Layer will be responsible for end of routing. This layer shall be available in all layered architectures for effective scalability.

4. **Layer 4** – End transport layer – Data movement to and from the thing is taken care by this layer. It should provide the compression of TCP/IP header with packet size 128B, IPv6 has 40B, UDP and ICMP has 4B. The layer should handle the packet fragmentation and reassembling. For low power devices frame size is 128 B, while Ipv6 requires MTU of 1280B. This mismatch has to be handled. It should support Mesh Routing, and PAN to

IPv6 (and vice versa) routing. It should be able to implement Internet protocol and transport protocol as per suggestions.

5. Layer 5 – Application / Presentation and QoS layer -Things are employed for tracking, tracing and controlling the required data and its environment. There can be any application at the Thing side. Things will simply transmit the generated data to end user's (mobile phones, laptops or PDAs) applications. As data is stored on the server, care shall be taken that this data is in a simple format and can be utilized by applications. Conversion of raw data to standard uniform format shall be made. E.g. XML or other simple formats are expected. This we can say as a presentation function.
6. Along with Five layer's own functionality, each layer should take care of following features
    1. Power consumption – Things are very small in size, having limitations in battery power and computing power. So at each layer care should be taken by various modules and protocols to save battery power and reduce as much less computing power as possible.
    2. Security – Things can be moving from one place to another place, and stays in foreign area with unknown nodes. Things can undergo a group of static and dynamic attacks. It is explained in chapter 2 and chapter five.
    3. Self awareness – Things shall be able to take protective or corrective action on its own.
    4. Event managers – Events can be triggered [11] for activating vertical handoff.
    5. Filters – are very much important to improve vertical scalability of the available resources in the architecture. Filtering should be before data dissemination and after data gathering.
    6. Scalability –can be easily scaled by taking care at the time of designing the modules and protocols.

4.4.2 Module requirement at different layers of Zigbee or Bluetooth Nodes

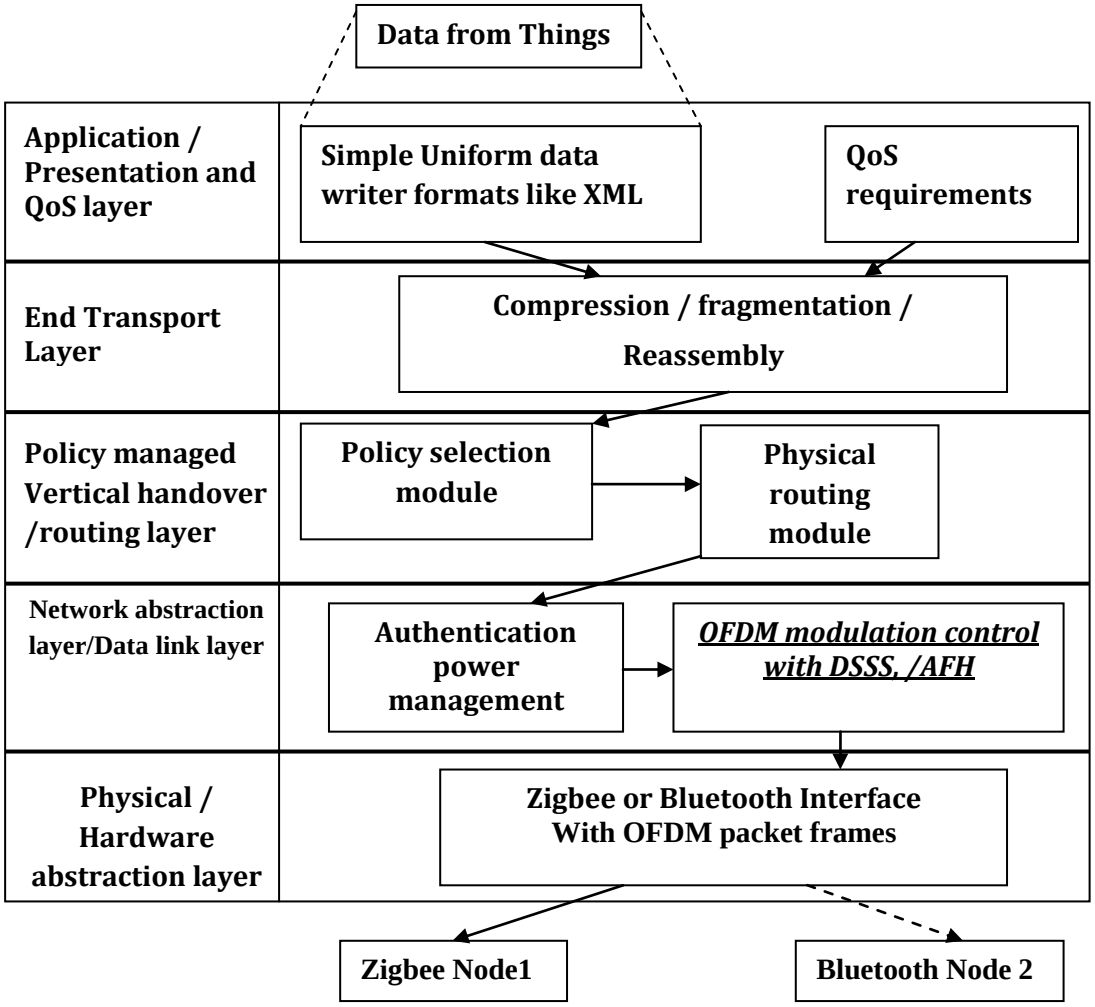


Fig 4-6: Component diagram / Modules present at typical IoT constrained Node of Zigbee or Bluetooth

The figure 4-6 displays the abstract overview of various modules present at all five layers of a Bluetooth or Zigbee node. The architecture will have any one technology either Zigbee or Bluetooth. Both node architectures are displayed here. At the TX and RX block of Zigbee, orthogonal polarization shall be applied with Antenna.

4.4.3 Modules requirement at different layers of BZ-Fi access point

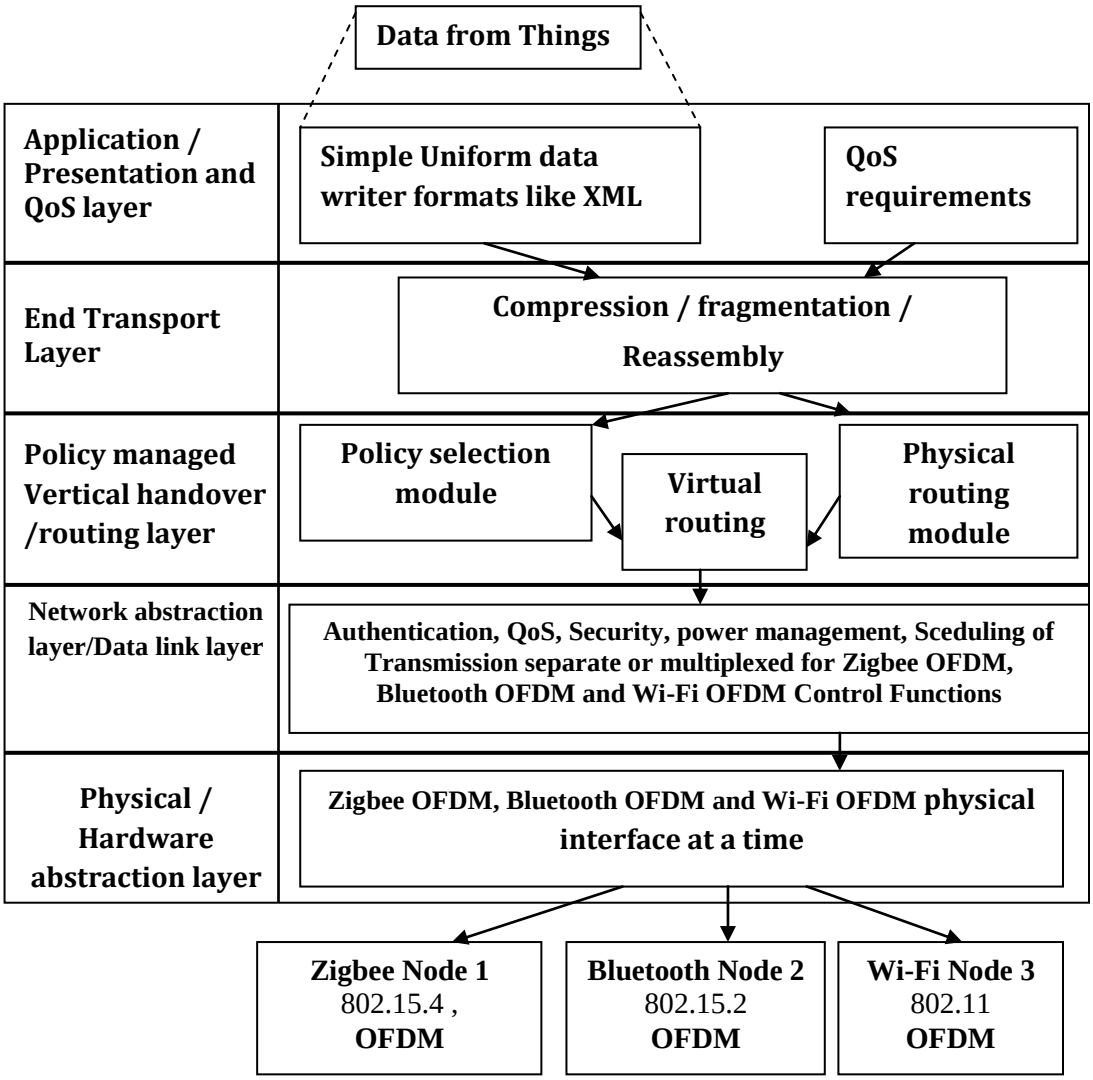


Fig 4-7: Component diagram / Modules present at BZ-Fi access point

Figure 4-7 represents various modules present at BZ-Fi access point. It will have interfaces of Zigbee, Bluetooth along with default Wi-Fi. These interfaces will be active at a time. Zigbee interface will transmit and receive packets perpendicular to Wi-Fi. Accordingly antenna polarization can be done.

We can say that this access point should help in heterogeneous interoperability of ISM operated technologies. In our case, our focus is only on Wi-Fi, Zigbee and Bluetooth. This can be a part of future stack which communicates to any heterogeneous stack.

4.4.4 Protocol stack for constrained nodes

In future it is expected that every node will talk to every other node, irrespective of the technology of the second node. Communication between heterogeneous nodes is expected. For such communication protocol stack [165] should be able to incorporate dynamic runtime modifications in protocol stack, its layers, and parameters. This modification is dependent on software architecture of protocol stack and it requires more memory. Modules of the same layer in two nodes communicate using protocols. Few example protocols are mentioned for each layer. There are many problems related with each layer. Some of them are covered under respective ones. The protocol stack is shown in figure 4-8. When Zigbee or Bluetooth node is present, respective protocol stack will be in action.

Application / Presentation and QoS layer

- According to heterogeneous networks QoS requirements, protocol shall be selected or designed for transmission.
- Binary Web Service protocol, Tiny Rest protocol, HTTP, With REST approach protocol
- SOAP,EXI, CoAP

CoAP limitations [166]

1. It is vulnerable to excessive traffics from sensor devices, as there is no authority to monitor and control the traffics. It works only with confined performance limit of traffic. It cannot work for bigger number of nodes traffics.
2. There exists security problem with its design. String URLs can have security risks due to complex processing on constrained micro-controller. It requires considering security concerns of header and other implications.
3. How protocol can take care of object security is still not clear.

End Transport Layer

- Network Services Protocol (NSP). This handles all the system independent aspects of logical links.
- UDP, µIP, LwIP- Applicable for connection and connection less protocol for Internet connection, IPv6/UDP stack– for interoperability.

Limitations [167]

There is not a single transport layer protocol which satisfactorily completes following requirements. Such as for handling multimedia traffic in constrained networks which takes care of congestion control, ability to handle high data rates with jitter, support for multipath

routing protocols. Event driven session creations and maintenance mechanisms, accurate data fragmentation and reassembly are few other features.

These limitations may be resolved because of OFDM implementation in Bluetooth and Zigbee.

Policy managed Vertical handover layer or network layer

Distance vector algorithms,

- 6LoWPAN Ad hoc Routing Protocol (LOAD), Dynamic MANET On-demand (DYMO) for 6LoWPAN, Hierarchical routing protocol is based on 16-bit short address.
- 6LoWPAN (Hi-Low), HIP, MIP, NIMO,SCTP
- Optimized Link State Routing Protocol (OLSR),path vector algorithm,
- GPRS Tunnelling Protocol

6LoWPAN Limitations [168-69]

1. Device mobility and scalability is another prime concern
2. The header overhead is large. Details are like 802.15.4 maximum frame overhead of 25 bytes, link-layer security can be as high as 21 bytes, 40-byte IP header, 8-byte UDP header and total comes to 94bytes. So for data only 33 bytes are left, which is too small. The relationship of header information to application payload is obviously really bad
3. Routing of packets in a mesh network is supported by 6LoWPAN Mesh Address Header. But other details of routing are left to link layer, which may create confusion resulting in unpredictable routing.
4. Maximum compression is possible for link-local addresses (for Pan Networks). It does not **support** for global addresses and is under progress.
5. Present 6LoWPAN nodes do not have to maintain compression state (stateless compression). But stateful compression of header is expected. Time limit for reassembly is only 60 seconds.

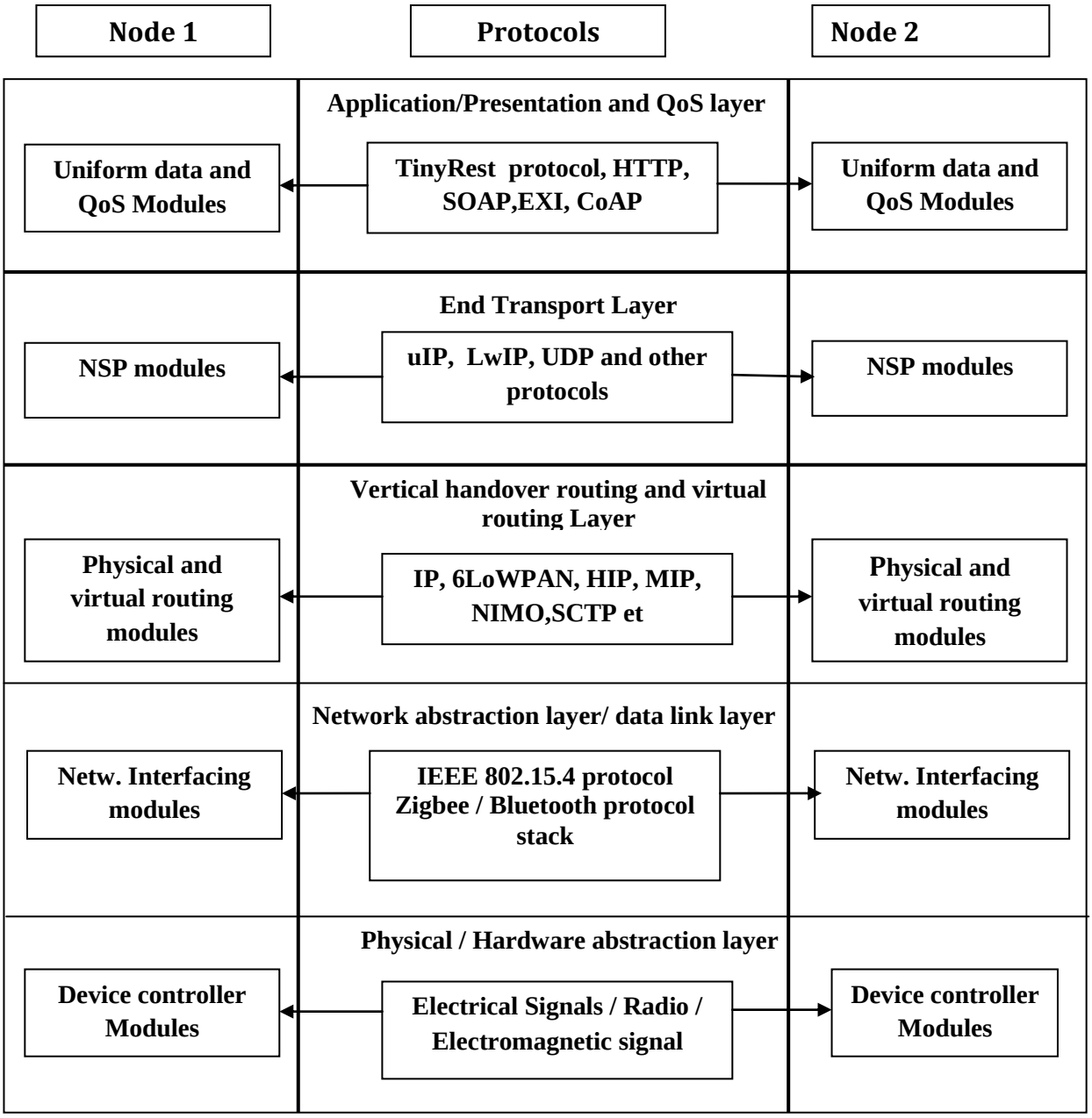


Fig4-8: Protocol stack for constrained nodes for HI

Network abstraction layer

- IEEE 802.15.4 –Ipv6 over Low power Wireless Personal Area Networks (6LOWPAN) protocols meant for the smallest devices with low power and limited computing powers.
- Bluetooth protocol stack – Includes Asynchronous Connection-oriented [logical transport] (ACL) , Link Management Protocol (LMP) , A/V Remote Control Profile

(AVRCP), Logical Link Control and Adaptation Protocol (L2CAP) , Radio Frequency Communications (RFCOMM) , adopted Bluetooth protocols and many more

- Zigbee protocols stack / Wi-Fi protocol stack.

Limitations [170-171]

1. Number of MAC protocols are available per applications e.g. S-MAC, T-MAC, DSMAC, D-MAC and many more. But they are not standardized and will vary as per application. Also Physical layer and sensor nodes are not standardized.
2. Instantaneous interference, channel contention, power constraints are some of the features need improvements.

Physical layer [172]

Primary requirement is that Zigbee, Bluetooth should support protocols for OFDM packet frame communication. They will be having OFDM features. But with scaled ones for Zigbee and Bluetooth. So existing protocols will not be applicable as they are. Completely new protocols are required to be designed.

4.5 Conclusions

HI architecture is proposed and completes the expected research goal requirements theoretically. Proposed logic for VHO with co-existence will allow simultaneous communication between all possible combinations of same or heterogeneous nodes of Bluetooth, Zigbee to Wi-Fi.

Proposed logic has two major contributions. First is design of proposed BZ-Fi access point. Second is the implementation of OFDM in Zigbee and Bluetooth.

BZ-Fi will eliminate huge number of gateways and helps in improving handover delays, which is a critical parameter at the time of call transfer. I.e. at the time of vertical or horizontal handoff. BZ- Fi access point will eliminate the need of VHO. All three networks will freely communicate to each other, acting like a single network.

Proposed research requires complete new set of protocols and stack. The resultant stack specifications may face problems of standardization. If contribution is found to be useful, standardization should not be a problem and new standard can be in picture.

Chapter 5

Security Architecture Design for Detection of All Types of Black and Grey holes

5.1 Introduction

Chapter works on the third non functional IoT architecture feature as security. The Internet of thing is a network of physical things, which can be stationary or movable. An Ad hoc network can be part of IoT. Mobile Ad-hoc networks (MANET) [173] can be dynamic and can be prone to a number of security problems. Legacy Internet systems and new Internet of Things, causes many security problems and lead to a big security framework. A mobile node becomes a foreign node for the fixed network. This foreign node can be really helpful in forwarding packets or maybe pretending to do so. The intentions of the foreign nodes are normally not clear and indirectly may make unsecure communication. If such a node exists, the network should provide basic and important security services such as availability, integrity, confidentiality, authenticity, and non repudiation. For this security services encryption, hashing, digital certificates, and digital signatures, etc can be applied as some of the mechanisms. Malicious nodes can cause isolation of nodes, or it can make starve node from connecting to its peer node, or even it may provide wrong or useless validations. Nodes, which pretend to co-operate and create problems in providing the correct destination path by giving wrong validations are called as malicious nodes in the grey hole attacks. Precautionary steps need to be taken against such malicious node attacks.

Few of these attacks are black hole, grey hole, and their co-operative attacks, which absorb all or some information in the form of packets. This leads to data loss. There are lots of detection and prevention mechanisms to stop such attacks of black and grey holes. All types of Black, Grey, and their co-operative hole attacks are still topics of research. A proposed algorithm is an extension of algorithm [174]. An algorithm reduces the number of tests conducted on all nodes engaged in transmission (some algorithms keep on checking the acknowledgements of received packets across all paths every time), and contributes in saving the battery life of constrained devices.

Section one outlines the chapter flow, and explains the basic concepts of security, grey, black, and co-operative grey holes and their behaviours. Chapter proposes a solution for the detection of grey and their co-operative attacks by using the Ad hoc On-Demand Distance Vector (AODV) protocol as a base protocol. AODV is considered because of its scalability, easy implementation, and efficient resource utilization. Section two, connects the legacy security framework with IoT framework. Framework tries to acquaint readers with all possible tasks required to be implemented for any type of security attack. Section three puts

the objectives in finding solution for the co-operative grey hole attack. State of the art of co-operative grey hole attack is made familiar in section four. Section five details three tests for all types of grey hole attack detection. Starting part of section discusses how our algorithm takes care of detection and makes difficult for attacker to find solution for continuation of attacks. Proposed algorithm, pseudo code, and simulation results along with the comparison with the algorithm [175], conclusions from results are gathered in the same section. Section six works further for providing security architecture for all types of grey hole attacks. Derived architecture can be used for authentication process of any DoS attack or any other attack.

Section two focuses existing security framework. Section four is a state of the art for grey hole detection. Section three, five six and seven are contributed by author. Algorithm is precisely applicable authentication of foreign node in any attack.

5.2 IoT Security Frame work

Table 5-I: IoT security framework [176]

Attack				
<----------Event----------→				
Tool	**Vulnerability**	**Action**	**Target**	**Unauthorized Results**
Physical attack	Design	Probe	Account	Increased access
Information Exchange	Implementation	Scan	Process	Disclosure of information
User command	Configuration	Flood	Data	Corruption of information
Script or program		Authenticate	Component	Denial of service
Autonomous Agent		Bypass	Node / Computer	Theft of resources
Toolkit		Spoof	Network	
Distributed tool		Read, Copy, Steal	Internetwork	
Data Tap		Modify, Del		

An IoT security is an action framework for preventing individual or a series of attacks. Operations of nodes and networks are composed of innumerable events. In security terms,

when events consist of some action taken against the target by a source to produce unauthorized results, they are called as attacks. An IoT security framework is nothing, but a base work or template provided for attack events for any type of network as available in table 5-I. An attack has the following parts of a framework as tools to exploit, and vulnerabilities to perform, an action, a target, and an unauthorized result.

5.3 Objectives of Security Architecture Design

By providing security architecture solution for grey hole co-operative attack detection, we contribute in IoT architecture design. Overall security attacks for the IoT are already discussed in chapter two. The objectives for IoT architecture are:

- To identify and study the various available protocol algorithms for Black, Grey, and their co-operative hole attacks
- Design and implement a network layer protocol for detection.
- Design a Network layer protocol for the same attack.
- From the above study, utilize the algorithm steps for security architecture design for any type of Black, Grey, and their Co-Operative hole (Denial of Service (DoS)) attack.

5.4 State Of The Art of Grey Hole and Co-Operative Attacks

A black hole malicious node replies falsely for any route request, without having any actual route or path to a specified destination. It receives all the packets from the source and drops all the received packets, instead of transmitting. When these malicious nodes support each other in a group, the attack becomes more serious causing bigger damage. Such a group attack is called as a cooperative black hole attack. A grey hole attack works similar to a black hole, but in a smart way. Grey hole initially works as a normal node, and then changes its behaviour for some time as attacker, and again starts behaving as a normal node. It drops data received from any node or, it may drop data for selective source, or it can be a combination of the above two symptoms. If such nodes are scattered in a co-operative manner, it is very difficult to find such a grey node. In both attacks, the network suffers from battery consumption and data loss. The proposed grey hole detection algorithm by default finds all types of black holes. Following are some of the protocols with the provision to prevent the black and grey hole attacks in a mobile Ad hoc Network. Table 5-II provides a detailed analysis of the previous research. It provides the techniques used, advantages, and disadvantages of the corresponding algorithm.

Routing Protocols for the prevention of Grey Hole Attack

Table 5-II: Comparison of various co-operative grey hole detection schemes.

Ref. NO.	Protocol Type-YR	Technique Used	Routing Reqmt.	Power Reqmt.	BW Reqmt.	Advantage	Disadvantages
174	AODV	End-to-end checking	Moderate	Moderate	Moderate	Help to detect chain of cooperating malicious nodes.	Backbone nodes evenly distributed across the network space.
175	2009	DRI (Data Routing Information) table maintained at each node	Moderate	Moderate	Moderate	Discover secure paths from source to destination by DELIVERY.	Here only foreign node is found out and no tests for grey holes are seen. No Simulation results are given----------
177	AODV 2010	RREQ in search of destination node but also in search of the restricted IP	----------	----------	More	Easy to detect the cooperative attack.	Nodes need to cooperate.
178	MAC Layered Type	Channel aware detection (CAD)	Moderate	More	More	Detect and isolate the selective forwarding attackers, Maximum PDR.	10% Packet loss
179	AODV Mar-12	Notification mechanism	Moderate	Moderate	Moderate	98.88% PDR	Nodes required to cooperate.
180 -81	DSR July 2010	2ACK Scheme	More	More	Less	Reduces additional overhead.	It works in only triplet.
182 -83	AODV 2011	Detection by source, destination and neighbours node	More	More	More	Detects the number of mistakes in identification	Nodes should always monitor to each other.
182 -83	AODV 2011	Watchdog Timer	More	Less	Less	This is simple method.	Each node should monitor to each other.
182 -83	AODV 2011	Local Collaboration and information cross validation	More	Moderate	Less	Each node uses a token, which authenticates the node in the networks.	Due to mobility of nodes mistakes in finding the malicious node increase
182 -83	AODV 2011	Additional node	Moderate	Moderate	Less	Nodes in a particular area are malicious node monitors only.	Assumes strong nodes are trustable.
182 -83	AODV 2011	Life cycle method	Moderate	Moderate	Moderate	Easy detection	Node needs to cooperate.
184	AODV 21 Feb 2012	Minimization technique	----------	----------	----------	Improve the performance and security.	Nodes need to cooperate to each other.

5.5 Proposed Solution for Co-operative Grey Hole Attack

The proposed solution is applicable to individual or to co-operative black hole, or grey hole attacks detection. The logic of RTC and CTS [185] and the DRI table acts as a base for implementation. As the frequency of dropping in grey hole behaviour is unpredictable, it is very difficult to find. It is expected that a malicious node will be detected through test 1 only.

The number of packets to be decided will be above the minimum thresh-hold value. This thresh-hold value can be set from minimum to maximum. The minimum value, we suggest is 10. Triple random testing is applied through the algorithm. We work with the Source node (SN), Destination node (DN), foreign node (FN), and Reliable foreign node (R_FN). F_RN is used to transmit the data, but has to undergo the tests till it becomes RN. Instead of testing all the neighbouring nodes and path nodes, only foreign and foreign reliable foreign nodes have to undergo the test. Three tests are as follows.

Tests 1- Random test packets - Packets for testing are sent randomly between say for e.g. 10-15 (any required number range can be set). The source node will send ten packets to a foreign node. RTS and CTS of both nodes are compared. If they don't match, it is decided whether the node is grey hole or not. Continuously, sending ten packets, serves to catch an unknown packet dropping frequency of a simple grey hole. When ten (required thresh hold) test packets are sent, checking is done for a normal or selective grey hole automatically.

Test 2- Random number of times test conduction -The test is carried out by a source node more than once randomly. After sufficient times testing is done, the individual source node will mark as a reliable node (RN), in its own DRI table. Till that time the foreign node has to undergo the test randomly and will be marked as (F_RN). It will become difficult for the grey hole attacker to decide the behaviour in a normal way as the test packet number is random. It can behave in its grey hole style, giving a chance for detection.

Test 3- Test 1 and test 2 for every new source node - Step one is conducted by every new source node with the same foreign node. As normal grey node detection will be completed in the first ten packets, but for the selective grey hole, every new source node has to check for itself. This continuous checking will detect the grey hole along with a selective grey hole, (for a new source) if it has escaped from the previous source node checking. This logic will sense all types of grey holes. The co-operative grey hole won't come into the picture as an individual foreign node is treated as an unreliable or foreign node (URN OR FN). All the above three steps in the logic make it sure, that 100 % all types of grey holes including co-operative detection is done.

5.5.1 Proposed Algorithm

The AODV [186] protocol acts as a base. Every foreign node has to undergo a test and then the CTS and RTS count is measured. Based on the RTS and CTS count, the behaviour of a node is decided. The algorithm logic is explained with the help of figure 5.2 and steps one to

three. Logic is applied on CGH (co- operative grey hole) part only, but it can be carried out for the lower CBH part also. Black and Blue paths are for reliable node (RN) paths. Red marked paths and nodes are the malicious node and co-operative path.

Step 1: Reliable path selection -–The source node wants to send packets to the destination node. It broadcasts the request to all the neighbour nodes in a network. CGH1and RN1 response to SN, that they have the path towards DN. RN1is a reliable node.CGH nodes are newly arrived nodes. So, they don't have any labelling in their DRI table as a reliable node. In this case, the path of RN1 is selected. Further, RN1 broadcasts for the path to DN. Again, a reliable node is selected for transmission. Node SN and RN1 (neighbouring nodes) mark in their own DRI table, CGH1 as new node. Proceeding further in the same manner, everywhere a reliable node will be selected for the transmission path and the other nodes will be stored as new nodes, till the destination node is reached. Priority is to transmit the data first, and then detection or verification of the new nodes. SN, RN1, RN2, RN3, Rn4, and DN are the nodes from selected path.

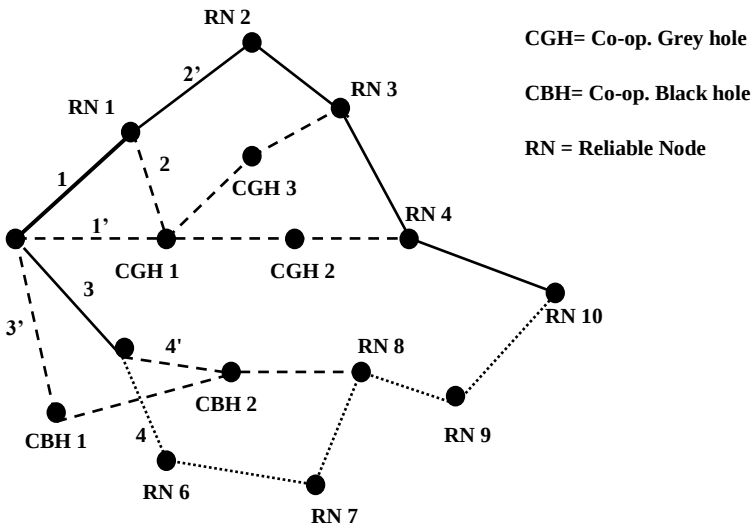


Fig. 5.2: Co-operative Black hole and Grey hole scenario.

Step 2: path selection for a foreign node: When a source node completes its transmission, it will select the path of foreign nodes purposefully. E.g. SN, CGH1, CGH3, RN3, RN4, and DN can be the other paths. This achieves two things. One, transmission is done without losing any packets. Second, the detection/verification of the CGH new node can be executed parallel to the other transmissions. This we can call as a police service operating parallel to the transmission. A test is carried out for CGH till the source node is confident, that it is not any type of grey node. If a foreign node undergoes the verification/ detection process for all

tests successfully, it will be marked as RN in their DRI table of source node only, or else it will be announced as a grey hole and removed from any future transmissions.

Step 3: detection process -The source node selects the path SN, CGH1, CGH2, RN4, and the destination node intentionally. SN sends the required packets to CGH1. A table will be maintained at each node for checking the number of transmitted and received packets using RTS and CTS. We check three cases of all co-operative grey hole attacks as follows i.e. simple grey hole, selective grey hole, and co-operative grey hole in simple or selective attacks.

3.1 Selective dropping - SN will transmit random packets continuously. If CGH1 is doing selective dropping for SN, it will drop all/or some packets. The nodes, which pass the tests, the source node will start using this node for its own transmission as R_FN. The source node will keep on testing the same reliable foreign node (R_FN) randomly in future. As per the check limit, in future the R_FN node is marked as a RN node in a source node DRI table, else will be omitted from transmission. After confirmation, the source node will start using this foreign node as a reliable node, for its own transmission. Here, the node is confirmed as a normal grey hole. The same foreign node again has to undergo the same test procedure for the selective grey hole by a new source node. Other nodes can't treat this node as a reliable node.

3.2 Complete Co-operative GH dropping – As no foreign node is considered for any transmission, the co-operative grey hole concept is eliminated. So, whether grey holes are scattered or cooperative, the same test becomes sufficient.

Table 5-III: Example of DRI table

Nodes	Transmitted packets by source	Received packets by Grey holes
CGH1(selective)	10	5
CGH2 (normal grey hole)	10	7
CGH3(Selective and normal)	10	2
CBG1	10	0
CBH2	10	0

5.5.2. Pseudo Code for Proposed Algorithm

```
SN -source node      DN- destination node      RN – reliable node      FN - new node      F_RN- Foreign reliable node
Y- Visit_no variable for random checking of a foreign node
X- Variable to decide test packets number randomly
Visit-no – variable tells how many times node is used for transmitting the data (stored in the DRI of the SN)
// random value is set for every new foreign (FN) or reliable foreign node (R_FN) under test in the start.

START

Y=0;                    // in every source node who is going to check for Visit_no test for FN in the beginning only
Node= SN broadcasts RREQ          // SN can be same or different for new transmission
Node receives RREP
While (Node!=DN)
{
Node broadcast RREQ
Node receives RREP
If( RREP is from F_RN and visit_no >50)                    // confirms completed testing successfully
        {       select the node in the path                // Convert F_RN to RN
                Node= RN (Next hop node)
        }
   Elseif (RREP is from RN)          // This time testing will not be done and data will be transmitted as if node is reliable
        {       select the node in the path
                Node= RN (Next hop node)
        }
    ElseIF (RREP is from FN)                               // node is FN and testing is done compulsorily
        {       Mark the node in SN DRI as  per test       //      Do the test first time
        }
    Else If (RREP is from F_RN and y<= Visit-no)// testing is done again as if it F_RN node has not completed its Visit_no
   testing
        { Mark the node in SN DRI as F_RN       //      Do the test last time
          Do test and continue the path selection}   // check again last time for confirming the reliable node test for random
checking

     Node =  RN (select 2nd RREQ node)                     // make RN as a source node for the next hop transmission
}
Transmit data with RN  and F_RN (if  > 50) nodes from SN to DN;       // complete data transmission with RN nodes first and
then start testing of intermediate detected foreign nodes which are marked in SN DRI table.

                                        Tests of foreign nodes

GOTO relative SN again;       // start of FN and R_FN testing
X= generate random number between 10 (min thresh-hold) to max thresh-hold to be deicide by programmer; // Test 1
Select the path of FN and F_RN purposefully

If (FN)
Y=  random Visit_no ( between Min to max);     // different  visit numbers are set  for every new foreign node – Test 2

For(i=0; i < X ; i++)
{ transmit all (random test packets from test 1) test packets to FN or R_FN
Visit_no ++;                                           // After all test packets are over, it is marked as one Visit_no.
}
      If ( RTS= CTS && CTS !=0)
         {
            If (FN)
           {
             Source node DRI table = reliable foreign node (F_RN) // Mark the foreign node temporarily as reliable foreign
node.
              Mark  visit_no in the DRI of the SN for visit to this F_RN
           }
          Else
            Increment  visit_no in the DRI of SN for this F_RN
         }
     Else if
{Announce it as a faulty node or grey node } ;
```

Fig 5- 3: Pseudo code for grey hole (all types) detection

5.5.3. Simulations:

The proposed and compared algorithms are implemented in the NS2. Simulation parameters set are as follows for algorithms.

Table 5-IV: NS2 Simulation Parameters for Grey Hole

Parameter	Explanation	Value
Simulation duration	total time of simulation for proposed algo.	1000ms
Simulation area	Area over which nodes are scattered	1000m X 1000 m
Number of mobile nodes	Total number of mobile sensor nodes	50
Transmission range	Communication ranges of a node	250 mtr
Movement model	nodes move randomly, normally used in ADHOC N/Ws	random way point
Maximum speed	speed of node movement in mtr/ms	4 m
Traffic type	Constant bit rate of packet traffic	cbr
Packet rate	maximum rate (in bps) at which the sender can send data along the link	0.5 se
Data payload	user data size	1000 bytes

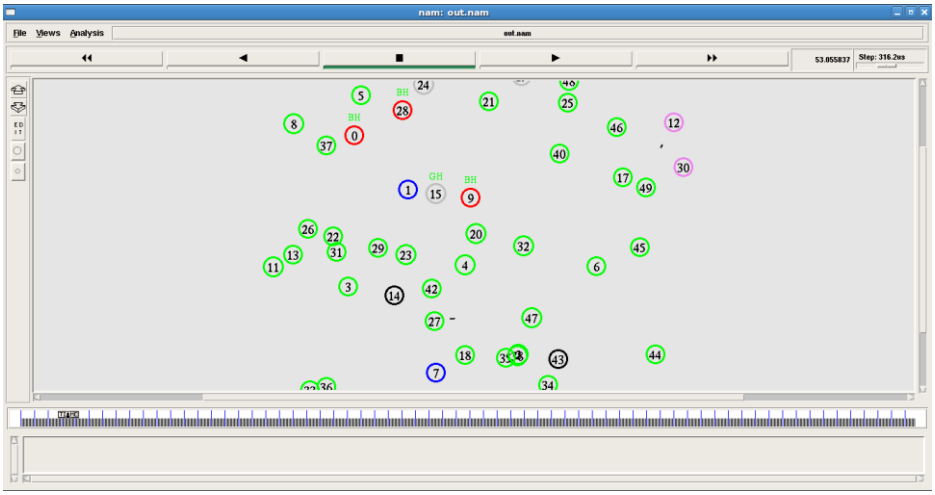


Fig 5-4: NS-2 Co-Operative Black and Grey Hole Scenario for Our Algorithm.

5.5.3 Results

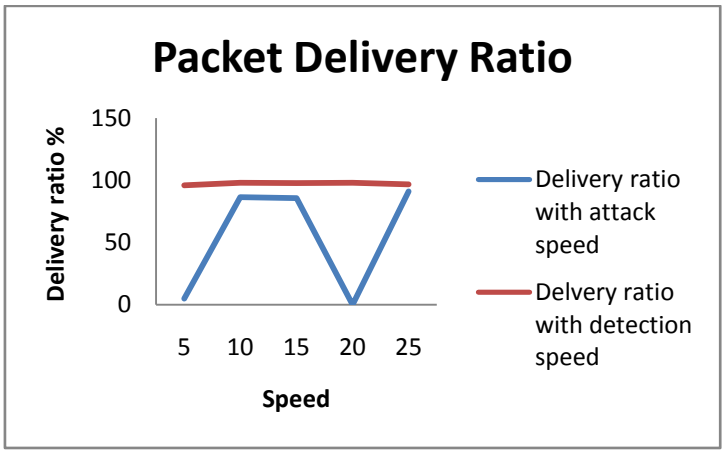


Fig 5-5: Effect of detection logic on PDR with speed

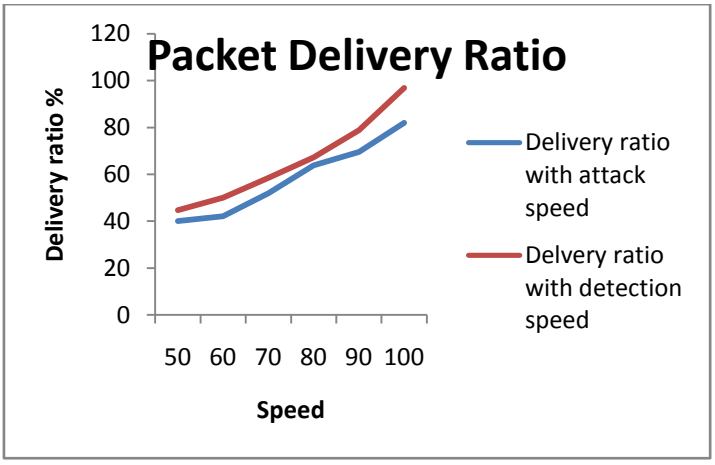


Fig. 5-6: Effect of detection logic on PDR with speed for other algo. [175].

5.5.4. Comparison: Paper [175] has proposed the algorithm for the Co-operative black and grey hole attacks. The algorithm is implemented and displays results in figure 5-5b and 5-6. Before starting the result comparison some of the other disadvantages are mentioned first. Topology wise one extra layer of network is required to be maintained. For single network it sounds ok. But considering IoT huge scope, it is not recommended. Also algorithm does not take into account, if such monitoring node itself can be malicious node. In that case any type of malicious node will not be detected. The back bone node is in monitoring mode only, where malicious node can fool this node also. The algorithm has become complicated as it requires one more protocols for co-ordination, between back bone nodes, source nodes and destination nodes. Intermediate back bone nodes, along with network nodes come in the data

transmission process. Number of such intermediate nodes and then monitoring nodes, also have to be checked for feedback of successful data transmission. In this checking, time complexity will be O (n). Back bone node shall check for malicious nodes from which data is dropped. Extra load is added with each data transmission in the form of prelude as number of blocks, encryption key, and random nonce.

At least once, data will be lost to some extent every time, when new malicious node becomes a part of network. Here time complexity is reduced to small extent, at the cost of loss of data once for every new transmission, if malicious node is present.

Our proposed algorithm is easy and simple to implement. It does not require any extra overload for data transmission (for testing purpose it is required, but not for data transmission). Data will not be lost in any transmission as foreign nodes are omitted from data transmission. As tests are carried out on only foreign nodes, less power will be wasted as compared with above algorithm. In our case time complexity comes out to be O (n) considering the path selection from source to destination. Number of test packets for repeated testing are going to be small, giving the effect of O (1) time complexity. Our algorithm does not provide logic of removal of detected malicious nodes, but with simple advertisement of such nodes, in the network, removal is possible.

Graph analysis infers following statistic

1. Our algorithm improves the packet delivery ratio with approximately 13 to 23% as compared with paper [171] algorithm as 3 to 8 % approximately. Improvement in the packet delivery ratio of algorithm [171] is increased up to 13 % at the end approximately. Our algorithm proves that the packet delivery ratio (PDR) is increased near to 100% which is not the case with algorithm [171].

5.5.4 Conclusions

From the graph we can conclude that in all cases, when the packet drop ratio is very high, with proposed logic it has been improved drastically. The overall ratio is maintained above ninety percent after applying the proposed detection algorithm. The delivery ratio is increased to near about 98 %. Time complexity of the proposed algorithm is O (1), as n is small.

5.6 Proposed Security Architecture for detection of black, grey and their co-operative attacks (selective, normal and combination of grey hole attacks)

All black and grey hole attacks are a kind of Denial of Service (DoS) attack. The attack is on routing or a network layer. But solutions can take place from the physical to the network layer. Security aspects concerned with all above attacks are:

- Authentication of a foreign node.
- Data confidentiality.
- Availability.

State of the art covers a number of defence and detection ways for these attacks. All are useful and are based on less or more utilization of node or network resources. But ultimately, we need to find a unique solution, which will take care of above attacks from the power consumption, traffic, and bandwidth point of view. Architecture requirements are as follows.

1. Security provisions at the source node shall be applied as much as possible.
2. Protocol should start using simple to complex algorithms. Time stamping logic at the start, which will eliminate the further checking of false replies of nodes. But a case can be there that, a malicious node is really near to the source node. Then further steps or logic should be applied.
3. Proposed algorithm shall be applied
4. There should be check points (police stations) in a network. These check points shall be of higher computing and battery power. Check points should not only monitor but test thoroughly the foreign node for all other types of Denial of Service (DoS) attacks, till it is proved to be safe. If possible foreign nodes should be kept isolated form static network transmission except for its own transmission.

The Encryption method with a smaller bit length is required to be found out. With the above guidelines the following software security architecture is proposed for a communication. The proposed algorithm is for authentication and authorization and accordingly, software architecture is proposed. It improves further, the availability and confidentiality of the data. Refer to figure 5-7a an5-7b.

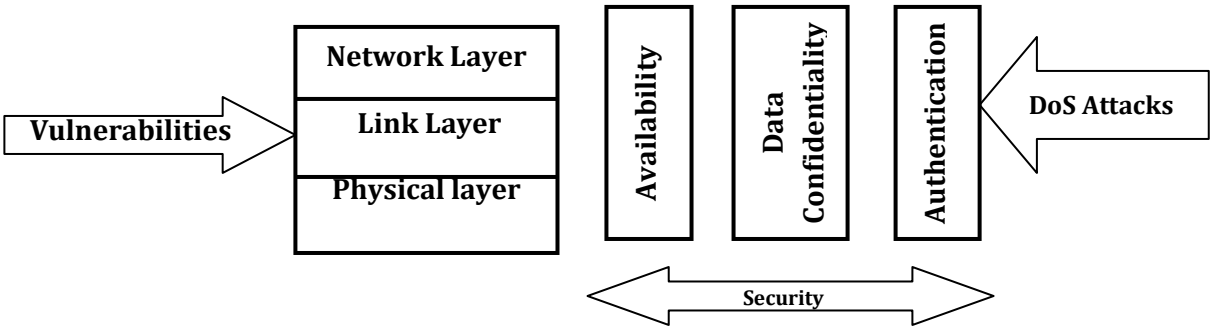


Fig 5-7a: Proposed Network Security Architecture for all types of Black and Grey holes.

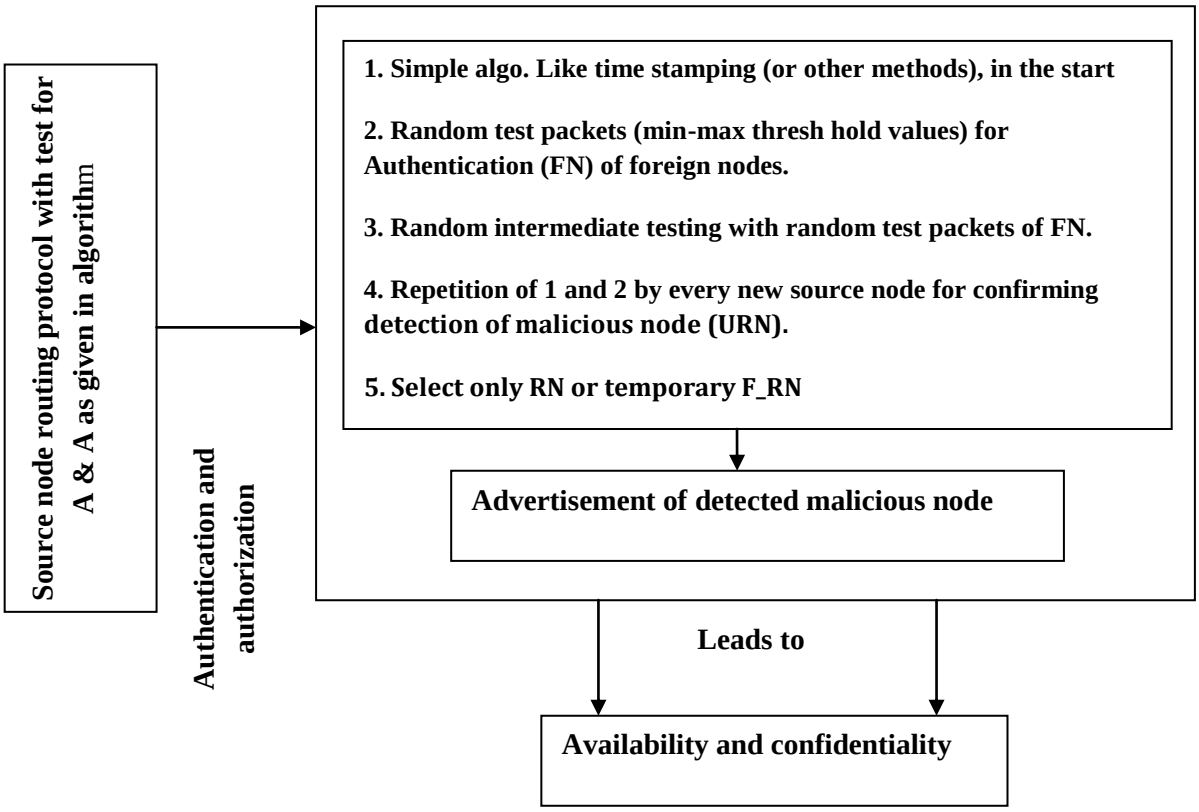


Fig 5-7b: Proposed Software Security Architecture for all types of Black and Grey holes.

5.7 Conclusions

Security architecture is proved practically for all types of grey holes. Authentication of any new node is must, in any type of network. Foreign nodes are like guests and should not be believed. Nodes of static networks should not employ foreign nodes as intermediate nodes for crucial applications data transfer. But static network nodes should help foreign node's data transmission and reception. Accordingly first classification of crucial and non crucial applications should be done.

The proposed authentication algorithm can be applied for any other attack, where authentication is required for foreign nodes.

Chapter 6

Internetwork means for IoT Architecture in RPC area

Part - A

Rural, Poor and Catastrophic ICT Area Definitions

6A.1 Introduction

The human is at the centre of Information and communication technology (ICT). Humans are living all over the world, in a scattered fashion. The World Bank data [187] confirms the poor number in one rural area as 70 % and another rural area as 50% of the total world. Normally areas are classified as urban, rural, and remote rural. With this classification, we can depict information about a population and its various aspects like the living standard, and education. The living standard denotes the infrastructure available in that area including communication. The basic facilities like education, medicine, and banking are missing in most of the rural areas. These facilities can be provided through the Internet. Information and communication technology will play a major role in the development of a rural area to some extent. The development can be in agriculture, irrigation, entertainment, and bringing the world nearer to the rural area. ICT definitions of the various areas have to be formed. These definitions will assist us in knowing the infrastructure available for communication technology. These defined areas will assist in giving firsthand information about the level of improvement we need to provide for education, medicine, and the banking sectors along with other applications. Every human from a rural and remote area has the right to meet the basic needs equally like the population from an urban area. The Institute of Prospective Technological Studies (Seville Spain) has developed the assessment model [188], which introduces a technological change in the rural area.

ICT solutions for RPC areas (Rural, Poor, Catastrophic areas) are the subjects of the research [189] including firm definitions and characteristics. There are various combinations of areas and a specific area may fall under all three categories. An ICT rural area is an area with no or low connectivity to the global ICT infrastructure compared with state of the art. An ICT poor area is characterised by the lack of affordable solutions compared with the potential needs and actual services provided. An ICT catastrophic area is an area where the availability of communication is degraded or not available due to a catastrophic event like cyclones, or an earthquake etc. Chapter points out that Okumura –Hata model is not sufficient for area definition, and the QoS behavioural patterns are also required. QoS behavioural patterns will help in specifying the respective area as rural, poor, catastrophic, or any other area as per the area matrix. .

Chapter out line is devised in figure 6A.1. Section one highlight the problems in RPC areas. Section contributes area classification from ICT point of view. Section two proposes new ICT area model using existing Okumura – Hata model.

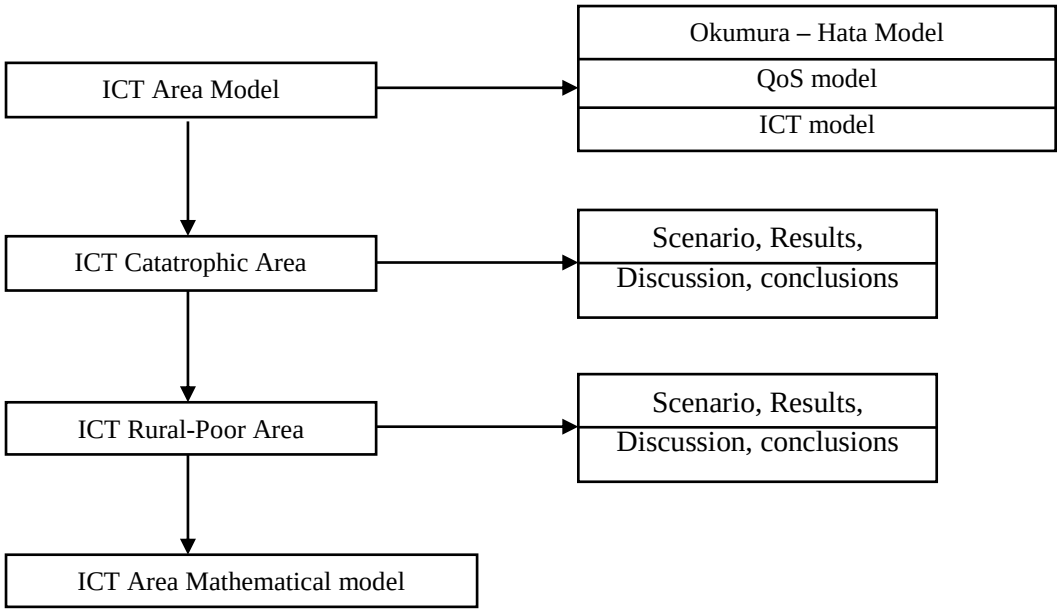


Fig 6A.1: Chapter flow diagram

Section three defines the catastrophic area with proposed ICT area model with one scenario as an example. Simulation results for QoS behaviour patterns, analysis and conclusions prove the same. Section four defines Rural-Poor areas with QoS behaviour patterns, analysis and conclusion, with topology as a next contribution. Section five provides mathematical model for ICT RPC areas. In the same section it is brought to notice that standardization of RPC areas in developing and developed countries is essential. All sections are contributions of thesis.

All sections are contributed by author. ICT area model emphasize the accuracy in finding specific ICT area. Definitions emphasize the shortcomings of specific area and provide readymade attributes for area enhancement.

6A.1.1 Drawback and Challenges

Although several rural broadband solutions exist, each has its own pitfalls and limitations [190]. Some choices are better than the others, but are dependent on how proactive the local phone company is about upgrading their rural technology. The chances of Infrastructure availability such as base stations, telephone networks, and others for communication (Internet of things) are lesser and one has to continue with the existing infrastructure along with new methods and ideas.

1. The main challenge with RPC areas are long distances for coverage in rural and repeated investments for Infrastructure in a catastrophic area respectively.
2. In the rural areas most essential services like education, health, and many more are still nonexistent. E-learning, E-medicine, E-banking, and E-agriculture services can

be provided. It is difficult to train people from these areas to use these applications/ services through ICT.

3. Power is not available in most areas, or even if present, it is unpredictable for its failure.
4. Skilled persons are required to maintain the infrastructure setup made for the ICT, but it is not so in this case.

6A.1.2 RPC Classification

Geographical areas and ICT areas differ from each other. While studying, it is noticed that rurality is relative. In an urban area we can also have a relative rural area. ICT areas can be classified as follows:

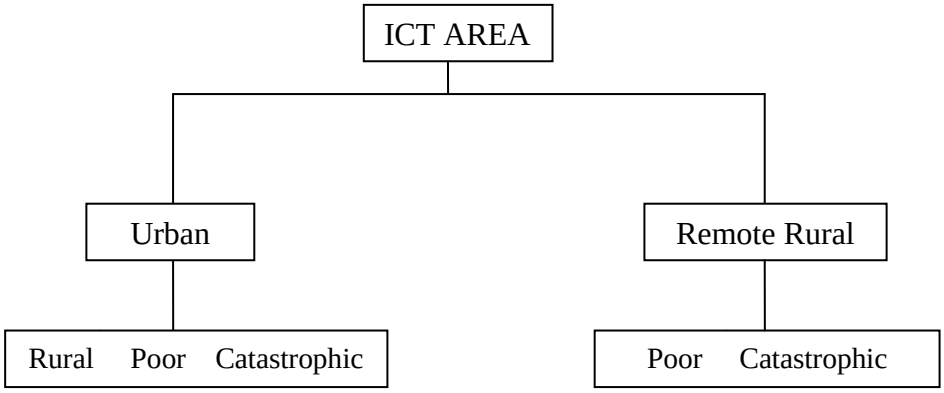


Fig 6A-2: Area Classification

There are various sub areas available as mentioned above. The following area matrix table 6A-I provides the possible combinations of various areas in one another. While reading, the row shall be read first and then the column area in it. For a possible correct combination, 1 is written or else 0.

Table 6A.I: Area Matrix

	Remote Rural	**Poor**	**Catastrophic**	**Urban**
Remote Rural	*1*	1	~~1~~	0
Poor	1	*1*	~~1~~	**1**
Catastrophic	~~1~~	~~1~~	*1*	1
Urban	0	**1**	1	*1*

The areas of interest are rural, poor, and a catastrophic area in any combination. Table 6A-I used only for showing these all possible combinations. As per combination, ICT area behaviour will change indicating state of the art and additional requirements for development. We can interpret the table as follows e.g. Rural area (first row) can have rural (default), poor, and catastrophic areas in it (first three columns), but it cannot have an urban area in it. Some

of the combinations represent same areas like rural –poor and poor- rural, rural – catastrophic and catastrophic – rural etc. These areas are represented with underlined, single or double stroked through number. Working on any one of these is sufficient. Diagonal area represents a single area and not a combination of two areas. They are represented with italic number. Zero in matrix indicates area combination is not possible at all.

6A.2 Proposed ICT Area Model

6A.2.1 ICT- Model

Information and communication technology can be better understood if we separate information and communication from each other, and try to understand each separately and then correlate them. Information is nothing, but data with intelligence or data with meaning. For example, 0 means off or false and 1 means on or true. When intelligence is added, this data becomes useful information. This data can be in the form of an image, audio, simple data, or a video form. Communication means the exchange of information from one entity to another thing for the required operations. These entities or Things can be one or many.

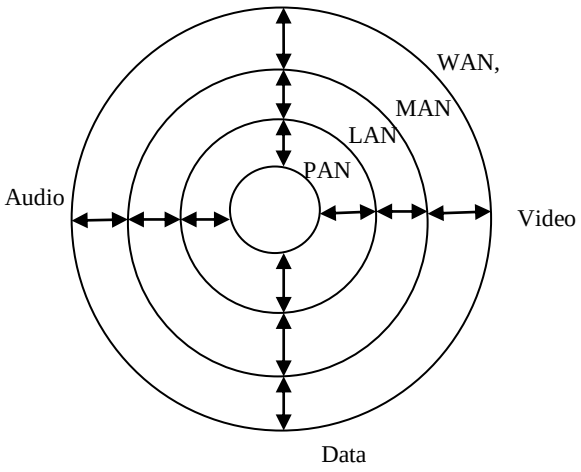


Figure 6A.3: Proposed ICT Model

These entities (Things) can be stationary in the same or various geographical locations or can be moving. Communication with these things is done through PAN, LAN, VAN, MAN, or WAN types of networks. Communication can be within the individual network or within intra network. When two or more different networks are connected we say that it is an internetwork. The internet is such a structured and organized system, which makes use of the above communication networks for exchanging information between them. This organized

information can be easily communicated to the user. These networks can exchange information between any network in any combination, for example, between PAN and WAN, or WAN AND WAN. The exchange of information can be for any application.

6A.2.2 Proposed ICT Area model

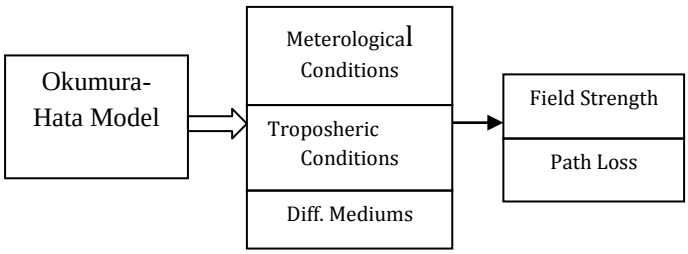


Figure 6A.4: Okumura-Hata Base Model

Normally, the model used for defining rurality is the Okumura Hata [191-192] model. We assume the Okumura Hata model (refer fig 6A.3) works with different mediums, tropospheric conditions, and meteorological conditions as a base for the definition of rurality. We call this model as a base model. For defining RPC areas, we are interested in the output field strength and the QoS behaviour pattern of the network (proposed model). According to network and place, the QOS values will vary.

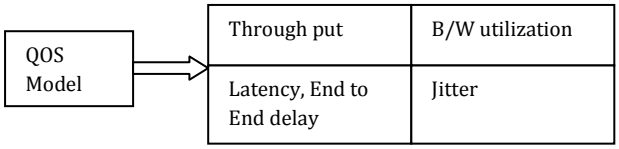


Figure 6A.5: QOS Model for network

Various QOS parameters can be taken into account further as traced in figure 6A.4.

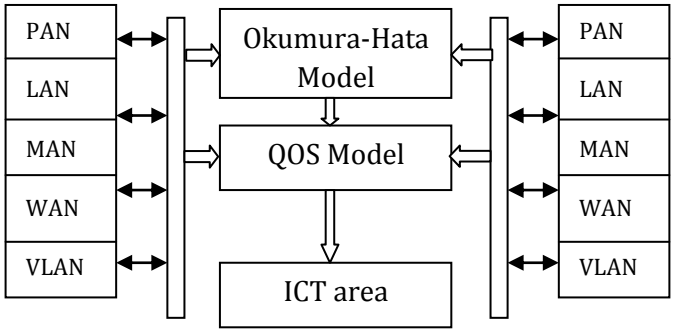


Figure 6A.6: Proposed ICT Area Model

Finally, the base model, QoS model (refer fig 6A.4), and ICT model are combined to get an ICT area model (Ref fig. 6A.5). For any area, the model will generate an intensity pattern,

and QoS patterns. By checking the results with the standard patterns of a country, the area can be decided.

6A.3 ICT Catastrophic Area

Almost every year, the world is struck by numerous catastrophes such as an earthquake, hurricane, typhoon, tsunami, etc. Catastrophic failures are the events, that cause the entire/most clusters of infrastructure, network partitioning, routers non-functional, and are inaccessible. Catastrophic failures can be natural or manmade such as terrorist attacks through software or physical damage. When a catastrophic natural disaster strikes, an organized and effective rescue operation is essential to rescue the victims who get trapped under collapsed buildings or landslides, and also to provide relief to those survivors who have lost their life support [193]. However, communication systems are usually paralyzed due to many causes. Due to the loss of communication systems, rescue and relief operations become extremely difficult, which leads to an unnecessary loss of many lives.

The causes of communication system failure can be base-stations crashed, trunks were broken, backup power generators failed, cooling systems for critical equipments failed, cell phones/ machines ran out of battery, chargers were not available, and communication network traffic jams and similarly many others. Threatened by so many sources of potential failure, there is a need for a reliable communication system to survive. When a disaster strikes suddenly, there is not enough time allowed to deploy a new fully-functional alternative solution. So, we can conclude that the communication system often fails due to natural or manmade catastrophes. This failure can be of different magnitudes according to the intensity of the catastrophes .The ICT catastrophic area is an area where the availability of communication is degraded or not available due to a catastrophic event like cyclones or an earthquake etc.

6A.3.2 Catastrophic Area Topology –Scenario

Proposed topology is a hypothetical Catastrophic Area. A simple topology has 50 nodes, and a UDP agent with a constant bit rate CBR traffic generator. The simulation runs for 110ms. The output is in trace file as out.tr and animation file as out.nam. The scenario is divided into 10 domains. 4 wirelesses and six wired. Three wireless domains have 15 nodes, and the fourth domain has 6A. The remaining domains consist of a total of 16 wired lines. These lines are connected to a base station, which is nothing, but a wireless node. There are a total of 12 base stations, which are scattered in 4 wireless domains.

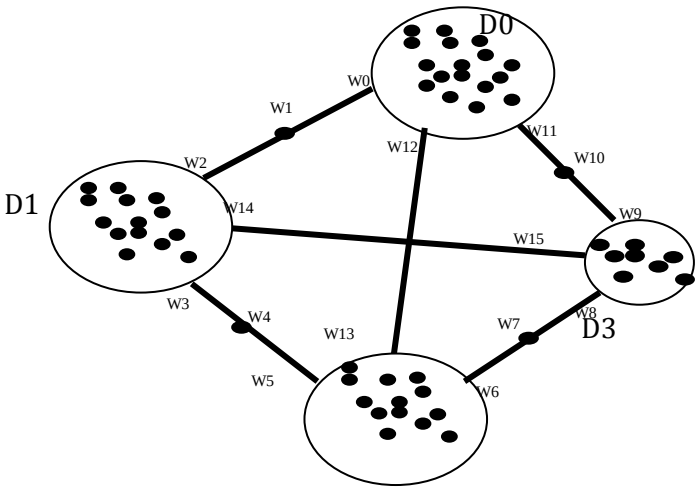


Figure 6A-7: Catastrophic Hybrid Model Topology Scenario

To study the catastrophic effect , the following steps have been taken.

1. Conectivity is provided between wireless-wireless, wired-wired, wireless-wired, and wired-wireless nodes. Various nodes from all the domains have been taken. The damage has been introduced by deactivating the links and nodes.
2. The graphs for the QoS patterns are plotted for the Normal connectivity pattern.
3. Domain 1 and 2 are damaged for 40-50 % and graphs for QoS patterns are plotted.
4. Domain 1, 2 and 3 are damaged for 90-92 % and graphs for QoS patterns are plotted .

6A.3.3 Results and Discussions

Readings are taken for packets generated, received, dropped, and lost packets. Average end to end delay, packet delivery ratio, and throughput are calculated from the above mentioned records. All the above mentioned and calculated results are plotted below.

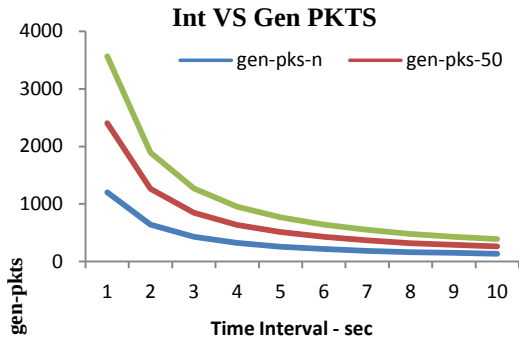


Fig. 6A-7a: Interval Vs Packets Generated

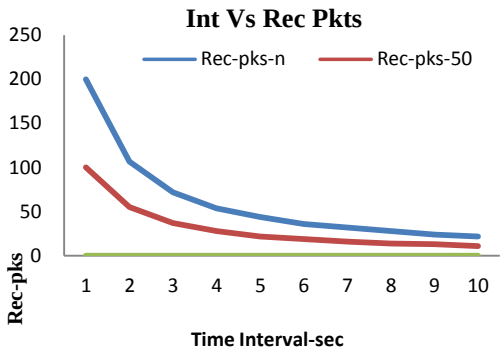
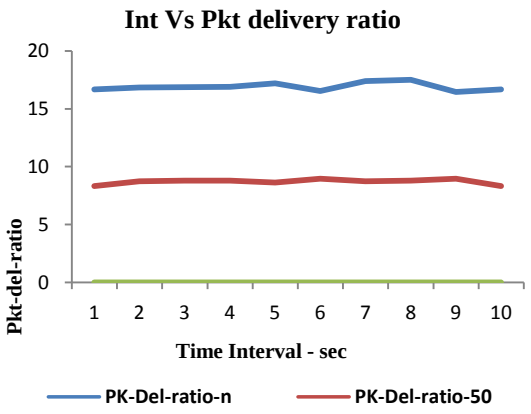


Fig 6A-7b: Interval Vs Packets Received

From the above graph (Fig.6A-7a) we can say that packet generation is there in all the three cases. This is because even if some nodes and wired links are made down, alive nodes from network still generate packets. The time interval suggests the effect of catastrophe on damage. Second graph (Figure6A-7b) indicates that the received packets are reduced as damage is increased. For 90 % damage no packets are received. Because of damage number of packets received will start reducing.



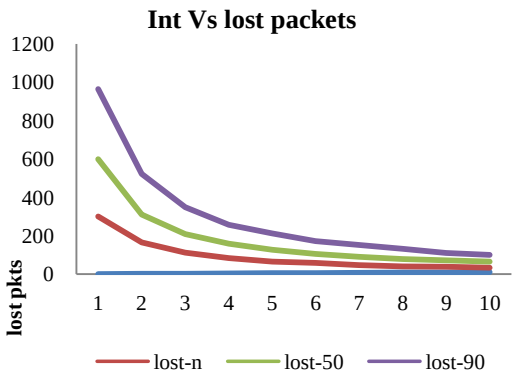


Fig. 6A- 7c: Interval Vs Packets Delivery Ratio Packets

Fig. 6A-7d: Interval Vs Lost Packet

Fourth graph (Fig. 6A-7c) is between the time interval Vs the packet delivery ratio. From the graph we conclude that the delivery ratio tends to zero with damage. From the graph (Fig. 6A-7d) we can say that packet loss ratio also increases as the damage is increased. Packets can also be lost because of congestion. Congestion is bound to be there when damages are there. Over the period of time network shall be trying to send packets though undamaged network which is working.

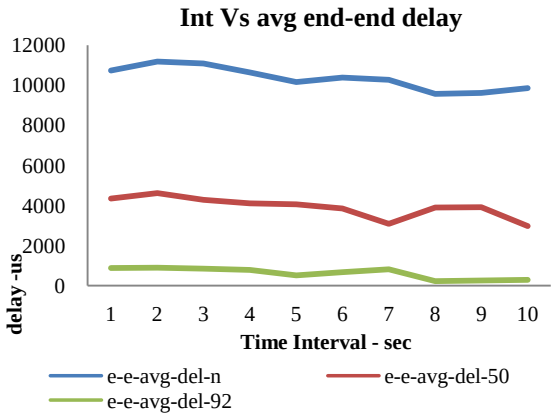


Fig. 6A-7e: Time interval Vs avg. end to end delay for a catastrophic area

The fifth graph (Fig. 6A-7e) is between the time interval Vs the average end to end delay. This is in usec. Because of the intermediate damages and congestion, the end to end delay that is latency is going to increase.

6A.3.4 Conclusions of Catastrophic ICT Model

It is observed that according to various topologies, the QOS parameters and values may change, but the overall graph nature remains the same. From the above graphs we conclude that whenever received packets are zero and the packet delivery rate is zero, there is a severe catastrophic condition. Here, we need to compare these results with normal results. The packet loss rate increases as the damage increases. A catastrophic condition can be due to a natural calamity or man made calamity.

6A.4 ICT Rural and Poor Area

6A.4.1 Topology-Scenario

Proposed topology is a hypothetical rural, and a poor area. A simple topology is created for urban, poor, and rural areas. A scenario (refer Fig. 6A-8) is created for the Hybrid model considering that the same is in practice, which is a combination of a wireless and a wired network. The nodes have two ray ground models and use the MAC-802.11 standard. The area for the model is set as 12786*100 in meters square. The total period of execution is 110ms. The antenna is Omni directional and in a drop tail type of queue. All these things can be changed and readings can be taken for other models, and queues etc. This script defines a simple topology of 82 nodes, and a single agent, and a UDP agent with a CBR traffic generator. Topology is divided into 13 domains. 7 wireless and 6 wired. Wireless domains have 20, 10, 10, 10, 10, 14, and 8 nodes each. All wired domains have two nodes each. These domains consist of a total of 6 wired lines. All the lines are connected to base stations from various domains, which are nothing, but wireless nodes. A total of 18 base stations are scattered in all wireless domains. The output is a trace file. Refer to the following topology 13. In domain D0 urban, poor, and urban rural effects are studied. D5 is at a very large distance from D0. This domain is worked as a remote rural area.

To study the required effect, the following steps have been taken.

1. Communication in an urban area is very much higher compared to the remote rural area. However, this communication varies from high to less at various places in an urban area. A Hugh communication area is termed as an urban area. The area with less communication is called as rural. In some parts of an urban area, transmission will be there, but not as a source or final destination. That is, no communication is generated and meant for these areas. They

are only intermediate means for commuting the information. Such areas can be called as urban poor areas. The scenarios reflecting the same conditions are created in the topology for urban, urban rural, and an urban poor area.

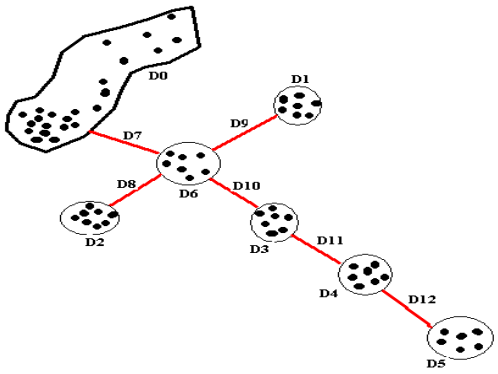


Fig. 6A-8: Scenario topology for a rural and a poor area

2. In a remote rural area on an average, less communication will be present than an urban rural area. The backhaul will be carrying information from many urban and rural areas on it. Intermediate communication between these areas will increase the load on the backhaul, and will lead to an increase in the end to end delay. Distance, number of towers, and various paths for backhaul available can be considered for a rural area. The same is generated through topology.

3. Transmission is generated between the various areas and within the area itself i.e. inter and intra domain.

6A.4.2Simulation results

Graphs are plotted for end to end delay versus generated / received packets, and throughput for downstream. In graphs GP= generated packets, RP= received packets, Thrput = throughput.

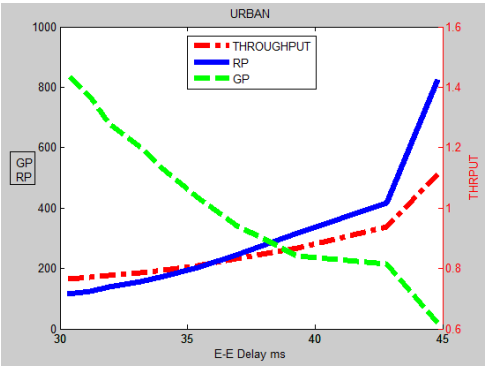


Fig. 6A-9a: Urban area QoS behavioural pattern

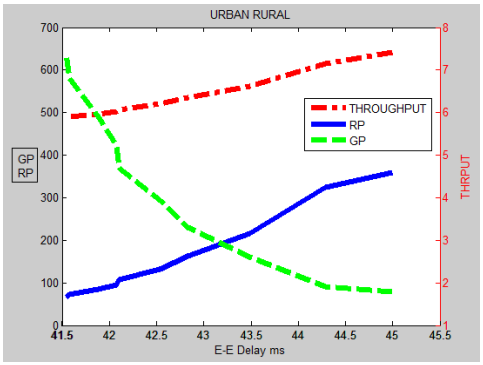


Fig. 6A-9b: Urban-rural Area QoS behavioural pattern

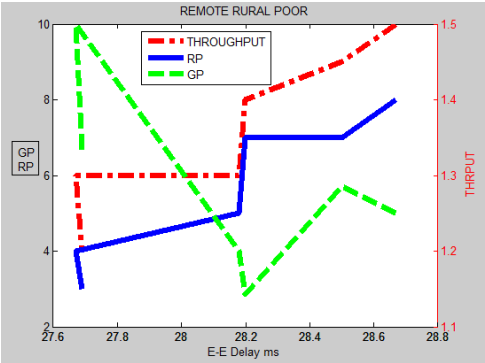


Fig. 6A-9c: Remote-rural area QoS behavioural pattern

Analysis – Rural area

1. As the source area is increased, more packets are generated.

2. Destination users in urban, urban rural and remote rural areas starts reducing leading to reduced received packets respectively.

3. As the resources are less utilized in a rural area, the throughput is in an increasing order.

4. E-E delay is increasing because of increasing distance, congestion, and limited resources.

5. Bandwidth utilization is directly proportional to the requirement of a particular area, and we can see that it is reducing from an urban to a remote rural area.

6. The number of resources like paths and base stations are reducing from an urban to a remote rural area leading to less bandwidth utilization, and bigger E-E delay.

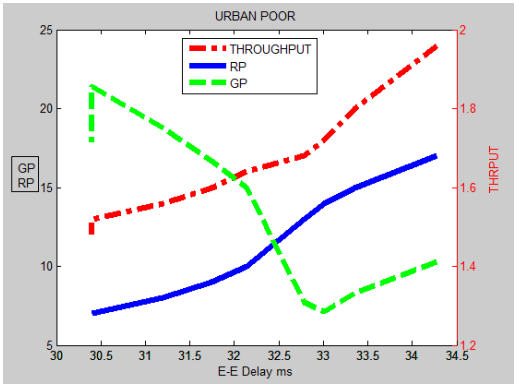


Fig. 6A-9d: Urban-poor area QoS pattern area

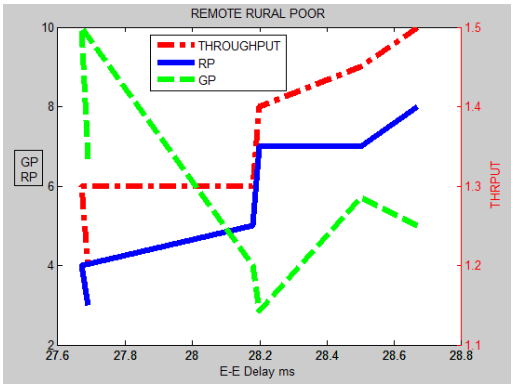


Fig. 6A-9e: Remote-rural –poor QoS pattern

Analysis – poor area

1. Gp for an urban poor area is very much less as compared to Gp of an urban and urban rural area. Gp and Rp are considered for source and destination areas only. Intermediate area Gp and Rp are not accounted. The results conclude that there is less communication, or no use of any e-applications.

2. Throughput and E-E delay are increasing.

3. Less utilization of the bandwidth for a remote poor area as compared to an urban poor area.

4. Infrastructure utilization is the same, for an urban, and an urban poor area, as it's an intermediate means. Same is the case with a remote rural and a remote rural poor area.

6A.4.3 Conclusion for RP area

The success of ICT is dependent on the utilization of an application by an individual, which in turn is dependent on the resources. For actual areas, the values of QoS parameters will be different, but the nature of graphs will remain the same. QoS parameters are taken for downstream, and can be taken for upstream also.

In general we can say that, all areas have their QoS parameters, which characterizes specific pattern. These patterns vary with an increase in the resources and the utilization of the applications related with them. An increase in utilization leads to the conversion of one area to another better ICT area i.e. Rural or poor to urban from the ICT point of view. As we have seen in an urban poor area Gp and Rp are very less irrespective of the resources. So, we can conclude that the utilization of ICT applications doesn't depend on the resources only.

6A.5 Mathematical model for ICT Areas

Mathematical modelling for RPC areas can demonstrate the relation between the various parameters. Area definition is a combination of the intensity pattern as per the Okumura - Hata Model [191-192] and the area QoS ICT model. A pattern is formed by a number of QoS parameters and in turn a number of equations for them. End to end delay, the number of resources, generated and received packets, distance, and the intensity pattern will be required.

Dimensional analysis is a mathematical technique, which makes use of dimensions as an aid to the solution of several engineering problems. All the parameters can be found out by an equation, composed of variables, which may or may not have dimensions. It helps in the systematic arrangement of physical relationships and the combining dimensional variables to form non dimensional parameters.

Any physical quantity can be expressed in terms of primary quantities as length, mass, and time. From these primary dimensions, the derived units are formed. We have used the following primary and derived dimensions. Other dimensionless variables are also mentioned in table 6A-II. RP, GP, and DP are expressed as b/s (bits/Sec), but its meaning is power generated, for received or dropped packets per sec. For power, the unit is Watt. Watt is expressed using primary quantities or dimensions as written in table 6A-II.

Relying Modelling of dimensional analysis was proposed by Lord Rayleigh in 1899.In this method a functional relationship of some variables is expressed in the form of an exponential equation, which can be dimensionally homogenous. Thus, if X is some function of variables X1, X2, X3……Xn; the functional equation can be written in the following general form

$$X = f(X1, X2, X3, ...Xn) \quad \text{..... (1)}$$

In this equation X is the dependent variable, while X1, X2, X3…..Xn are independent variables. The above equation can be expressed as

$$X = C(X1^{a} x2^{b} X3^{c} .....Xn^{n}) \quad \text{..... (2)}$$

Where C is a dimension less constant. The exponents a, b, and c are then evaluated on the basis that the equation is dimensionally homogeneous. The dimensionless parameters a, b and c are then formed by grouping together the variables with like powers.

Area definition is nothing, but finding out the various ranges of QoS parameters from, which it is made up of. Area function can be written as follows.

$$Area = f(E, BW, E-Ed, GP, RP, Nt, Np, Nn) \quad \text{..... (3)}$$

Nt, Np, Nn are dimensionless variables.

E- Intensity as per the Okumura-Hata model and other variables are mentioned in table II.

Table 6A-II: Primary and derived dimensions for area definitions

Quantity Name	**Symbol**	**Dimensions in L-M- T**	**Unit of measurement**
E-E delay	E-Ed	$L^0 M^0 S^1$	S
Congestion	C	$L^0 M^0 S^0$	Erlag dimension less constant
Received Packets	RP	$L^2 M^1 S^{-3}$	$M^2Kg S^{-3}$
Generated packets	GP	$L^2 M^1 S^{-3}$	$M^2Kg S^{-3}$
Dropped packets	DP	$L^2 M^1 S^{-3}$	$M^2Kg S^{-3}$
Bandwidth	BW	$L^2 M^1 S^{-3}$	$M^2Kg S^{-3}$
Distance between source and destination	D	$L^1 M^0 S^0$	M
Mass	M	$L^0 M^1 S^0$	Kg
No. of Base Stations	Nt	$L^0 M^0 S^0$	-
No. of paths	Np	$L^0 M^0 S^0$	-
No. of nodes	Nn	$L^0 M^0 S^0$	-
No. of users	Nu	$L^0 M^0 S^0$	-

Equations E-Ed, GP, and RP are derived below using the Rayleigh dimensional analysis method. In this method, the functional relationship of variables is expressed in the form of an exponential equation, which is dimensionally homogeneous.

End-End delay (E-Ed) can play a major role in an area QoS pattern. It is dependent on congestion (C), distance (d) between source and destination, band width (B/W), number of paths (Np), number of towers (Nt), and the number of nodes (Nn) at a source and at a destination separately. We can write for ($E\text{-}E_d$),

$$E\text{-}Ed = f(d, BW, M, C, Np, Nt) \quad \text{(4)}$$

By using the Relying Modelling we get the equation as

$$E\text{-}Ed = K\left[\left(d^{2/3}\right)\left(BW^{-1/3}\right)\left(M^{1/3}\right), \frac{1}{Nt}, \frac{1}{Np}\right] \quad \text{(5)}$$

The second parameter is generated packets in an area. It is dependent on the number of nodes in a specific area, speed of packet generation Sp, number of nodes Nn at a source, and the number of users. It focuses on the source side. The function Gp is

$$GP = f(Sp, Nn, Nu) \quad \text{(6)}$$

By using the Relying Modelling we get the equation as

$$GP = K(Sp, Nn, Nu) \quad \text{(7)}$$

The third parameter is received packets in an area. This focuses on the intermediate infrastructure and the related parameters along with the destination side. The number of packets may be dropped intermediately because of infrastructure and congestion. The number of users will be less in a rural, poor, and a catastrophic area. So, it is, but natural that the received packets will be lesser.

$$RP = f(Gp, Dp, C, Nt, Np) \quad \text{(8)}$$

By using the Relying Modelling we get the equation as

$$RP = K\left[\left(\frac{Gp^2}{Dp}\right), C, Nt, Np\right] \quad \text{(9)}$$

Congestion is dependent on the number of hardware resources available, individual resources, processing capabilities, bandwidth, number of nodes, and power availability. It doesn't have any unit or dimension and the constant is known as Erlag. K is a dimensionless constant in all equations, which has to be found out from experiments. The distance can be equated as

$$D = \sqrt{(x2 - x1)^2 + (y2 - y1)^2} \quad \text{(10)}$$

Where (x1, y1) are the co-ordinates of a reference location of the city, and (x2, y2) are the destination co-ordinates. All the above equations will yield values of QoS parameters

according to the area. There has to be some standard range available. By looking at, which, one can say that a various set of values correspond to a rural, poor, or catastrophic area. Following are some of the ranges found out from the NS2 simulator.

An exercise is carried out for fixing the various ranges for deciding the area type hypothetically. From the above observations of the graph of a rural and a poor area we can decide the various ranges for area standardisation for downstream for simulated topology. For deciding the ranges for area, we assume 1000 max packets are received in an urban area. All the ranges have been fixed up from an urban area range of values as a base line or reference. Considering 25 % extra in the above value, the ranges are fixed up. When answers from the QoS parameters and the equations or the actual values recorded on field, fit into the ranges of table 6A-III, we can say that the QoS pattern is for an urban, or rural, or any other area.

Table 6A-III: Hypothetical ranges for area definition standardization

Area	RP %	E-E delay us	B/w Utilization %	No. Of Paths Np	No. of Base stations
Urban	85- 15	56-41	25-5	4	3
Urban rural	40-8	56-53	10- 2	1	2
Remote Rural	15-2	60-44	5 – 0.50	1	1
Urban poor	0.2-0.1	13-2.5	0.5 – 0.2	4	3
Rural poor	0.1-0.05	15-3	0.25- 0.1	1	1

From table IV the remote rural poor area can be defined as having 0.1-0.05% RP, 15-3 us E-E delay, bandwidth utilization is in 0.25-0.1 %, Np and Nt is 1. In the same way the other areas can be defined with the help of the corresponding QoS ranges from the above table.

6A.5.1 Need of Area Definition Standardization

All countries in the world have urban, rural, and catastrophic areas. These countries can be divided into developed and developing countries. Any area definition indicates the vision of area needs, facilities available, ICT infrastructure available, businesses available, and the required investment. All these aspects are to be taken into consideration. Researchers, private or government service providers shall understand the scope or requirement for the basic and advanced development, and business in it. Researchers will get background information for

technologies applied and problems for invention. For example, in a rural area long distances are a major problem. This is indirectly related with the investment. The above information indirectly presents the living standard of the respective area.

The objective of any country's policy for rural area development will support to overcome the challenges, the population of such areas is facing and to utilize their potential. The best example is of EU's policy [193-194]. Only saying the area name is not sufficient, but the sub areas also have to be taken into consideration, as mentioned in the area matrix table 6A-I.

Basic needs for ICT areas definition standardization are as follows:-

1. To provide a clear vision of the basic needs required in the development of rural and poor areas with e-learning, e-medicine, and the e-banking point of view.
2. To provide a clear picture of the research, efforts are required to be carried out for the development of rural, poor, and catastrophic areas.
3. To minimize the time and money in the all operations right from installation to maintenance.
4. To envisage a clear vision for the investments required for the development by the government or individuals.

For standardization of table V ranges, a systematic approach is required. As the actual QoS values (PR, GP, E-E delay etc.) for a specific area are not available to the individual. Standardization for these patterns is a must. A survey has to be made to find out these ranges for all the areas and then these ranges are required to be fixed up for the developing and developed countries areas. Table 6A-IV lists all the points for standardization.

Table 6A-IV: Required standardization parameters for an RPC area

Parameter Name	Standardization required for Rural, Poor, and Catastrophic
QoS pattern parameters 1.Delay e-e 2. Through put 3. Generated packets 4. Received packets 5. Bandwidth Available 6. Bandwidth utilized	1. Value Ranges for all rural area combinations as per the Area matrix. 2. For all the parameters of column one. 3. Ranges for catastrophic severity e.g. above 90%, and 50%. For all the parameters of column one.
1. Nodes and their computing power. 2. Base stations.	1. Number range in all rural, poor, and catastrophic areas. Area combinations as per the Area matrix. 2. For all the parameters of column one.
Power	Availability and load shed ding time if it is there.

6A.5.2. Conclusions

RPC ICT areas are mathematically modelled as well as proved practically with limitations of realistic behaviour patterns. QoS patterns are plotted with hypothetical topologies. An individual cannot get the required data. The activity shall be carried out with the help of governments, and standardization bodies to get the real QoS patterns.

Chapter 6

Internetwork means for IoT Architecture in RPC area

Part - B

Outdoor Visible Light Wireless Communication

6-B.1 Introduction

Out of many communication technologies available, thesis fixes the application of Visible light communication (VLC) in the rural and catastrophic areas as a first aid for IoT. These areas suffer from investments on long distance coverage and repeated investments in the catastrophic area, and a fast erection of network and connection to network for communication. The proposed logic uses handy cam for data transmission and reception for long distance. When catastrophe occurs, people do not have any network setup. Using handy cam available or can be given through helicopter, communication network can be erected and established in very short duration. Handy cam is not utilized before, for long distance applications. The concept has been proposed and proved with experimentation. Results validates that for long distance outdoor VLC on-off keying, can be used for solving above challenges. As per the speed of transmission, various IoT applications can be developed.

VLC can be applied for point to point communication (back-haul) as well as for broadcasting. The proposed VLC is an economical and fast (no special time) solution in all aspects, like very low maintenance cost, and no highly skilled and technical persons are required. The VLC network can be erected by a layman. A line of sight is required, (if the line of sight is disturbed, by snowfall and rainfall, and may result in loss of data) and a transmitter and receiver are required to be fixed at higher heights, are some of the disadvantages.

Section two puts forward a state of the art for VLC. Section three is handed by author and proposes the connectivity means with easily available handy cam and high speed camera. Section four provides results of communication for high and low speed. Section five concludes finally

6B.2 State of the Art

VLC is proved using analogue communication for 13 KM [195]. A camera is also used for vehicular outdoor communication [196] for short (40-60m) distances. Papers [197-198] contribute in state of the art of VLC for indoor applications. We have implemented the OOK technique using a video camera for a long distance of (1.5 KM) outdoor because of limitation on availability of the High speed camera.

6B.3 Proposed Model

The main objective of our experiment is to establish wireless communication using visible light for outdoor to prove the concept.

1. Introduction to wireless visible light communication for outdoor using on-off keying (OOK).
2. Testing communication at various speeds and distances.
3. An analysis of the received data using MATLAB.

We have designed and developed a transmitter with a PIC microcontroller based circuit and a LED bank (of five LEDs) with a high switching rate. A video camera is operated as a receiver (Sony handy cam and Motion Pro). The transmitter and receiver (refer fig 6B.1) should be placed at a height (in the real case). The data bit stream is continuously transmitted and captured with various speeds and received with the video camera. The video camera is interfaced to the PC to receive data from the camera. This data is processed further with the Mat lab image processing tool and the final data stream is extracted from the receiver.

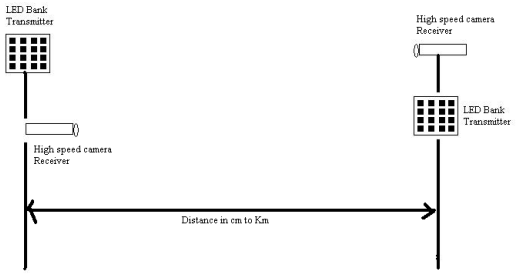


Fig 6B.1: VLC wireless communication Model using Handy cam

The image capturing device captures the status of the LED light in the form of an intensity between 0 -255. We have implemented it as black and white. The thresh-hold value is decided with the help of experimental results at various times and distances. A LED ON is recorded as digital high and LED OFF is recorded as digital low.

A. System Block Diagram

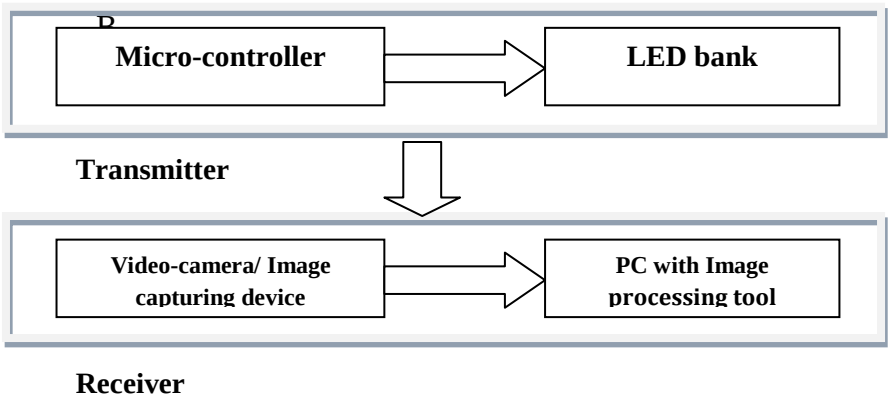


Fig.6B.2 system block diagram

Figure 6B.2 shows the block diagram of the design it comprises of microcontroller, LED bank at transmitter and video camera, PC at the receiver end. In our case we have used

video camera, but any image capturing device can be used. CMOS image sensor, which has feature of selecting any pixel for data is more ideal device. Image processing tool as such not required for final product. Transmitter has different part like micro-controller (PIC16F877A), current booster, and LED bank. Micro-controller is used to transmit different data streams at required speeds. Selected PIC uC operates at 40 MHz. The switching rate of power LEDs are up to 1us. This switching rate can provide us to communicate up to 1,000,000 bits per second. Power LED is required for brightness of light, so that it can be captured from long distance. Current requirement of power LED (350mA) is more than the of output current at the micro-controller (25mA). Current booster circuit is added for the same. The LED bank is seen as a single source of light from a long distance.

The yearly power consumption of the bank is (5*24*365)/1000 Kwh, which comes to 44Kwh approximately. The light weight outdoor access point consumes (50*24*365)/1000, which is 438 Kwh. This indicates huge power saving by VLC. Table 6B-I displays results of experiments with various speed and distances.

6B.4 Results

6B.4.1. LOW SPEED RESULT (SONY Handy CAM) 25FPS

Fig 6B.3a: LED OFF original

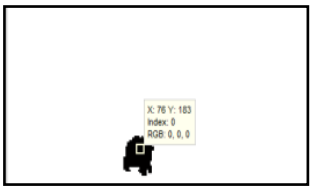


Fig 6B.3b: LED OFF post video frame processing through MATLAB.

Fig 6B.3d: LED ON original

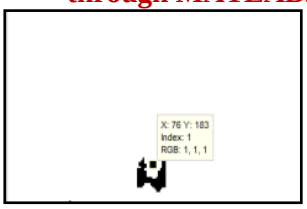


Fig 6B.3c:LED OFF Post video frame processing through MATLAB.

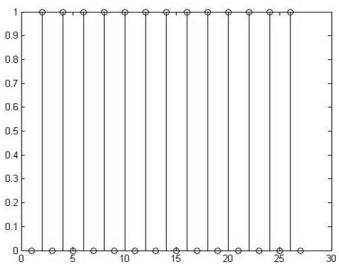


Fig 6B.3e: Plot of the variable bit value (k)

Figures 6B.3a to 6B.3d are taken at a distance of *1.5* Km from transmitter, at 6.30 pm evening with sony handycam. Figures 6B.3e represents the decoded image from Matlab.

6B.4.2. Low Speed- From 0.5Km at 12 AM

Results are taken at day time. In a day time day night mode was turned on. The intensities received are 114, 233, 99, 206, 96, 213, 57, 232, 44, 223, 51, 232, 38, 207, 34, 227, 40, 235, 60, 229, and 102. From these intensities we decided that 140 (pixel intensity) as a thresh hold value for deciding transmitted data as 1 or 0.

6B.4.3 HIGH SPEED RESULT (MOTIONPRO IDT Y4-S2) 128,000 fps

Figure 6B.4 shows indoor high speed experimental setup results.

Fig.6B.4: Experiment setup

Figure 6B.4 shows indoor high speed experimental results.

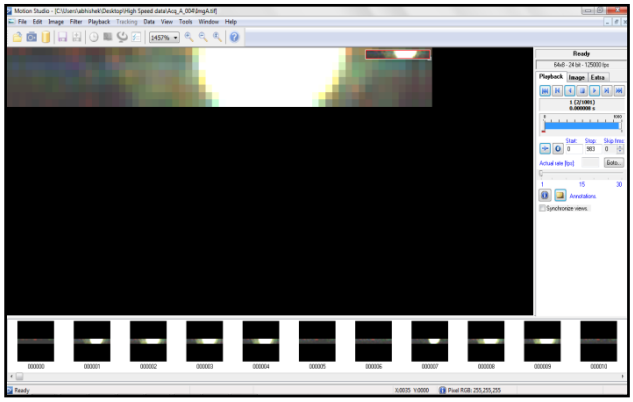


Fig6B.5: Images from Motion Pro

Fig 6B.6a: LED OFF state

Fig 6B.6b:LED OFF state

(processed through MATLAB)
(original video frame)

Fig 6B.6c: LED ON state

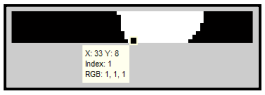


Fig 6B.6d: LED ON state
(processed through MATLAB)
(original video frame)

Figures 6B.6a to 6B.6d are taken at a distance of 1.5 Km from transmitter, at 7.30 pm evening with sony handycam. Figures 6B.6e represents the decoded image from Matlab.

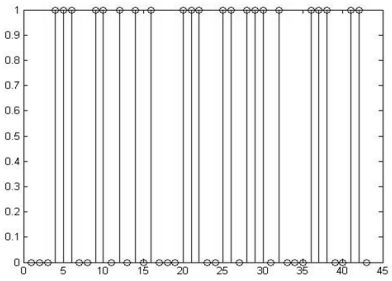


Fig 6B.6e: Plot of the variable bit value (k)

From the plot we can see that the data received is (000111001101010100011100110111010001111...and so on).

Table 6B-I: Summary of Experiment results

Sr. No	Place	Time	Distance	Speed fps	TX data	RX data
1	Out-door	7.30 Pm	1.5 Km	25	101010....	101010....
2	Out-door	12 AM	0.5 Km	25	101010....	101010....
3.	In-door	12 AM	1m	100,000	0001110011010101	0001110011010101

6B.5 Conclusions

Visible light communication for outdoor applications with simple camera is proved practically. There is no need of special hardware in emergency. In our experiment we used white light, but red, green, or blue colour lights can also be considered.

The required distances (m to hundreds of Kms) can be covered by using lenses of various sensitivity. IoT applications can be implemented with the use of normal, economic lenses for short range applications.

Chapter 7

Conclusions and Future Scope

7.1 Conclusions

IoT dream's first step is completed by scaling of TCP/IP to 8 bit microcontroller. Many issues like scalability, power consumption, heterogeneous interoperability and security etc. are still not answered completely. Unless and until basic all requirements of IoT are complete, IoT architecture cannot be complete.

Thesis designs IoT abstract system, software and HI networking architecture theoretically. Core IoT architecture is validated. Proposed software architecture should serve for any IoT application. Abstract generic IoT architecture is applicable for standard objects or Things.

Architecture's vertical scalability can be achieved by reducing or suppressing data at source level, without affecting the final data output. When IoT application has same reading or value as previously sent, data can be omitted from transmission. Number of processes at various stages, related to this data transmission or reception will be reduced or eliminated causing for scalability. Other techniques can be found out further for sending bigger data in a single byte like packed BCD. This reduction or omission of data causes vertical scalability of power consumption, traffic congestion, QoS parameters, memory storage, fast discovery services and many more. This technique is applicable to any software, system or network architecture, but it is more suitable for IoT applications, as IoT applications have small size, fixed, repeated data for transmission Scalability solution will result in improving huge energy consumptions.

Co-existence of Wi-Fi, Bluetooth and Zigbee (ISM band technologies) is an IoT requirement. Current research in ultra low power CMOS devices will permit implementation of OFDM, in Zigbee and Bluetooth. The implementation may lead to new standard requirement. Use of OFDM will reduce the interference in co-existence. Proposed solution for heterogeneous interoperable network architecture is expected to improve speed of data transmission for constrained devices along with very less interference.

Detection of all types of grey hole attacks (indirectly all black hole attacks also) are possible to near about 100% without causing transmission delays. The packet drop rate is improved to near about 95 percent, excluding atmospheric losses. Designed security architecture is useful for any type of DoS attack's authentication and authorization.

Chapter 6 concludes that Okumura-Hata model is not sufficient for defining area, but the proposed ICT area model is required additionally for the same. Even proposed ICT area model can be sufficient for finding out any type of area. Hypothetical rural, poor and catastrophic area QoS behaviour patterns obtained from simulations, are not exactly same as

real ones. Real data has to be collected from the service providers or from the governments. Without their help it is not possible for individual ones to collect data and define QoS ranges for RPC areas. Developed and developing countries will have various QoS behaviour patterns for RPC ICT areas. It is very much required, to standardize these definitions or patterns.

Chapter 7 concludes that VLC can be used as a first aid communication means for outdoor rural and catastrophic areas with the help of easily available handy cam. It can be used as backhaul or peripheral network communication technology.

Conclusion can be drawn that architecture perspectives like scalability, heterogeneous interoperability, data volumes, and security features are interrelated with each other. As scalability increases, data volume also increases leading to storage and data searching problems. More security of data will be required with scalability and heterogeneous interoperability. Various types of nodes may be moving from one place to another causing HI. Identifying intentions, detection and prevention of these attacks is cumbersome.

7.2 Future Scope

There is a huge scope for research in the Internet of Things domain. Open issues and challenges other than the architecture are detailed in chapter two. Related with the thesis research few are mentioned below.

1. As per Zacman's matrix other views of IoT architectures should be worked further.
2. Development of code for software IoT architecture, system reference IoT generic architecture with suggested modules (figure 3-2) on respective layers can be worked further.
3. Validation and verification is required to be done further.
4. Transreceiver for Bluetooth using OFDM has to be designed and implemented.
5. Transreceiver for Zigbee using OFDM has to be designed and implemented.
6. Implementation of BZ-Fi access point shall be done after points three and four are completed.
7. The heterogeneous Interoperability for data, services can be worked further for same three technologies.
8. The heterogeneous protocol which makes communication between any two network technologies possible is required to be worked.
9. All features like horizontal and vertical scalability, security, interoperability, device adaptability, power consumption, and data volume shall be worked further.

10. More effective ideas are required for the data compression techniques at the source or the IoT node level. Different data storage techniques should be researched further.
11. The business process modelling of the IoT is not done yet successfully. Developing BPMN tools for the sensor node modelling is also a topic of research.
12. Finding an encryption key with the small number of bits for security is a big challenge for the IoT networks. This invention will help in the prevention of all attacks.
13. VLC provides solution to problem of connectivity of Rural and Catastrophic areas. There is critical problem of power consumption in RPC areas and should be solved for IoT.

References

[1] N. Gershenfeld, R. Krikorian, D. Cohen, The internet of things Scientific American 291 (4) (2004) 76–81

[2] http://cordis.europa.eu/search/index.cfm?fuseaction=news.document&N_RCN=30283

[3] http://services.future-internet.eu/images/1/16/A4_Things_Haller.pdf

[4] "Deploying RFID - Challenges, Solutions, and Open Issues", book edited by Cristina Turcu, ISBN 978-953-307-380-4, Published: August 17, 2011 under CC BY-NC-SA 3.0 license

[5] EPOSS, E. ETP EPOSS IOT Definition. 2011. Available online: http://old.smart-systemsintegration.org/internet-of-things/Internet-of-Things in 2020 EC-EPoSS Workshop Report -2008 v3.pdf/download

[6] Jongwoo Sung; Sanchez Lopez, T.; Daeyoung Kim; " The EPC Sensor Network for RFID and WSN Integration Infrastructure Pervasive Computing and Communications Workshops, 2007. PerCom, Workshops '07. Fifth Annual IEEE International Conference

[7] The EPCglobal Architecture Framework, EPCglobal Final Version 1.3, Approved 19 March 2009, <www.epcglobalinc.org>

[8] Luigi Atzoria, , Antonio Ierab, , Giacomo Morabito, "The Internet of Things: A survey," Computer Networks, volume 54, Issue 15, 28 October 2010, Pages 2787–2805

[9] Daniele Miorandi, et al., "Survey Internet of things: Vision, applications and research challenges," Ad Hoc Networks, Volume 10 Issue 7, September, 2012, Pages: 1497-1516

[10] Strategic Research Roadmap by European commission, 15 SEPTEMBER, 2009. ••• The meaning of things , ec.europa.eu/information_society/policy/rfid/documents/in_cerp.pdf

[11] http://www.charuaggarwal.net/IoT.pdf (book chapter)

[12] Valipour, M.H.; Amirzafari, B.; Maleki, K.N.; Daneshpour, N., "A brief survey of software architecture concepts and service oriented architecture "Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference

[13] Larosa, Y.T.; Jiann-Liang Chen; Yi-Wei Ma; Sy-Yen Kuo "Socio-organism inspired model forming multi-level computational scheme for integrated IoT service architecture" Future Internet Communications (BCFIC), 2012 2nd Baltic Congress on ,Publication Year: 2012 , Page(s): 68 – 71

[14] Dominique Guinard, ,VladTrifa, , FriedemannMattern , Erik Wilde, "From the Internet of Things to the Web of Things: Resource-oriented Architecture and Best Practices" Book

[15] Pascal Urien, HervéChabanne, Mathieu Bouet , E. Gressier-Soudan , "HIP tags privacy architecture Oriented Architecture for the Web of Things" Systems and Networks Communications, 2008. ICSNC '08. 3rd International Conference on, Digital Object Identifier: 10.1109/ICSNC.2008.21 Publication Year: 2008 , Page(s): 179 - 184

[16] RenDuan; Xiaojiang Chen; Tianzhang Xing "A QoS Architecture for IOT, "Internet of Things, (iThings/ CPSCom), 2011 International Conference on and 4th International Conference on, Cyber, Physical and Social Computing, Digital Object Identifier 10.1109/iThings/CPSCom.2011.12,Publication Year: 2011, Page(s) 717 – 720

[17] J. Internet of Things - Architecture, ―SOTA report on existing integration frameworks/ architectures for WSN, RFID and other emerging IoT related technologies –wrt to requirements, IoT-A Internal Report, IR1.2, December 2010

[18] Huansheng Ning and Ziou Wang, "Future Internet of Things Architecture: Like Mankind Neural System or Social Organizati on Framework?",CommunicationsLetters,IEEE Volume:15, Issue:4, DigitalObject identifier:10.1109/LCOMM.2011.022411.110120,Publication Year: 2011 , Page(s): 461 - 463

[19] Tao Yan, Qiaoyan Wen. "A Secure Mobile RFID Architecture for the Internet of Things "Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on Digital Object Identifier: 10.1109/ICITIS.2010.5689514, Publication Year: 2010 , Page(s): 616 - 619

[20] Jia Shen, Xiangyou LU, Huafei Li, Fei XU, "Heterogeneous Multi-Layer Access and RRM for the Internet of Things "Communications and Networking in China (CHINACOM), 2010 5th International ICST Conference on, Publication Year: 2010 , Page(s): 1 - 5

[21] Bin Xu, Yangguang Liu, Xiaoqi He Yanping Tao, "On the Architecture and Address Mapping Mechanism of IoT "Intelligent Systems and Knowledge Engineering (ISKE), 2010 International Conference on Digital Object Identifier: 10.1109/ISKE.2010.5680775 , Publication Year: 2010 , Page(s): 678 - 682

[22] Haitao Pu, Jinjiao Lin, Fasheng Liu, Lizhen Cui, "An Intelligent Interaction System Architecture of the Internet of Things Based on Context" Pervasive Computing and Applications (ICPCA), 2010 5th International Conference on, Digital Object Identifier: 10.1109/ICPCA.2010.5704136 , Publication Year: 2010 , Page(s): 402 - 405

[23] Urien, P. ; Elrharbi, S. ; Nyamy, D. ; Chabanne, H. ; Icart, T. ;Pepin, C. ; Bouet, M. ; Cunha, D. ; Guyot, V. ; Krzanik, P. ;Susini, J.-F. "HIP-tags, a new paradigm for the Internet Of Things" Wireless Days, 2008. WD'08.1st IFIP , Digital Identifier: 10.1109/WD.2008.4812927 , Publication Year: 2008 , Page(s): 1 – 5

References

[24] Angelo P. Castellanit, Nicola Buit, Paolo Casari, Michele Rossi, Zach Shelby, Michele Zorzit, " Architecture and Protocols for the Internet of Things: A Case Study" Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on , Digital Object Identifier: 10.1109/ PERCOMW. 2010.5470520 , Publication Year: 2010 , Page(s):678-683

[25] Sundmaeker, H.; Kovacikova, T.; "CuteLoop - An Approach for Networked Devices Enabled Intelligence" Software Engineering Advances (ICSEA), 2010 Fifth International Conference on, at Nice ,E-ISBN: 978-0- 7695-4144-0

[26] www.smart-rfid.eu

[27] www.traser-project.eu

[28] Anggorjati, B.; C□etin, K.; Mihovska, A.; Prasad, N.R.;"RFID Added Value Sensing Capabilities: European Advances in Integrated RFID-WSN Middleware" Sensor Mesh and Ad Hoc Communications and Networks (SECON), 2010 7th Annual IEEE Communications Society Conference on Digital Object Identifier: 10.1109/SECON.2010.5508231 ,Publication Year: 2010 , Page(s): 1 – 3-ASPIRE

[29] Akram, H.; Hoffmann, M.; "Laws of Identity in Ambient Environments: The HYDRA Approach " Mobile Ubiquitous Computing, Systems, Services and Technologies, 2008. UBICOMM '08. The Second International Conference on Digital Object Identifier: 10.1109/UBICOMM.2008.89 Publication Year: 2008 , Page(s): 367 – 373

[30] Akram, H.; Hoffmann, M.; "Supports for Identity Management in Ambient Environments - The Hydra Approach " Systems and Networks Communications, 2008. ICSNC '08. 3rd International Conference on ,Digital Object Identifier: 10.1109/ICSNC.2008.77 ,Publication Year: 2008 , Page(s): 371 - 377.,

[31] Klaus Pavlik , R&D Environment "RFID is a key technology in the fields of ICT for the European industry. Although no longer an emerging technology, the breadth of its potential.",..2008, The RFID Roadmap: The Next Steps for Europe, Pages 141-174-stolpan

[32] Eldor Walk, Alexander Gauby and Frank Neubauer, "Standards, a vital instrument for new technologies to avoid an uncontrolled growth of research results. Standards regarding RFID concern frequencies, communication, data, networks, safety and applications ", 2008, The RFID Roadmap: The Next Steps for Europe, Pages 15-45 –GRIEFS

[33] Palattella, M, Accettura N,,Vilajosana X, Watteyne T,,Grieco L, Boggia G, Dohler, M " Standardized Protocol Stack for The Internet of (Important) Things , Communications Surveys & Tutorials, IEEE , Issue: 99, Publication Year: 2012 , Page(s): 1 - 18

[34] Zhiyan Liu ; Bao Xi ; Yuan, Y." Analysis on IoT Communication Protocol", Information and Automation (ICIA), 2012 International Conference on, Publication Year: 2012 , Page(s): 126 – 130

[35] Raza, S. ; Trabalza, D. ; Voigt, T. " 6LoWPAN Compressed DTLS for CoAP" Distributed Computing in Sensor Systems (DCOSS),, 2012 IEEE 8th International conference on,Publication Year: 2012 , Page(s): 287 - 289

[36] Internet of Things - Architecture, ―SOTA of Communication Protocols by Application Areas, IoT-A Internal Report, IR3.1, December 2010.

[37] R. Stewart et al., "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", Request for Comments 5061, Internet Engineering Task Force, September 2007.

[38] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture", Request for Comments 4423, Internet Engineering Task Force, May 2006.

[39] http://www.can-cia.org/index.php?id=170

[40] http://www.profibus.com/

[41] http://www.odva.org/Home/ODVATECHNOLOGIES/tabid/64/lng/en-US/language/en-US/Default.aspx

[42] http://knx.org

[43] http://www.lonmark.org/

[44] K. Leung, G. Dommety, V. Narayanan and A. Petrescu, " Network Mobility (NEMO) Extensions for Mobile IPv4", Request for Comments 5177, Internet Engineering Task Force, April 2008.

[45] E. Nordmark, M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", Request for Comments 5533, Internet Engineering Task Force, June 2009.

[46] IETF Internet DRAFT core CoAP 03, ―Constrained Application Protocol (CoAP), October 2010.

[47] IETF RFC 4919, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," August 2007. Addressing

[48] Adam Dunkels. Full TCP/IP for 8 Bit Architectures. In Proceedings of the First ACM/Usenix International Conference on Mobile Systems, Applications and Services, (MobiSys 2003), San Francisco, May 2003

[49] IETF ROLL Internet Draft, ―RPL: Routing protocol for low power and lossy networks, draft-ietf-roll-rpl-14, October 2010.

[50] IETF RFC 5673, ―Industrial Routing Requirements in Low-Power and Lossy Networks, October 2009.

[51] IETF RFC 5826, ―Home Automation Routing Requirements in Low-Power and Lossy, Networks, April 2010.
[52] IETF RFC 5867, ―Building Automation Routing Requirements in Low-Power and Lossy, Networks, June 2010.
[53] Glenford E. Mapp, FatemaShaikh, David Cottingham, Jon Crowcrof "Y-Comm: A Global Architecture for HeterogeneousNetworking "Invited Paper, WICON '07: Proceedings of the 3rd international conference on Wireless internet , October 2007
[54] Bin Xu, Yangguang Liu, XiaoqiHeYanping Tao, "On the Architecture and Address Mapping Mechanism of IoT "Intelligent Systems and Knowledge Engineering (ISKE), 2010 International Conference on Digital Object Identifier: 10.1109/ISKE.2010.5680775 Publication Year: 2010 , Page(s): 678 - 682
[55] Gerhard P. Hancke. Security of Proximity Identification Systems. PhD thesis, University of Cambridge, Cambridge, United Kingdom, February 2008.
[56] IlanKirschenbaum and Avishai Wool. How to Build a Low-Cost, Extended-Range RFID Skimmer. Cryptology ePrint Archive, Report 2006/054, 2006.
[57] M.R. Rieback, G.N. Gaydadjiev, B. Crispo, R.F.H. Hofman, A.S. Tanenbaum "A Platform for RFID Security and Privacy Administration" 20th USENIX/SAGE Large Installation System Administration conference (LISA 2006), Washington DC, December 2006.
[58] C. Krishna Kumar, G. Jai Arul Jose, C. Sajeev, and C. Suyambulingom," SAFETY MEASURES AGAINST MAN-IN-THE-MIDDLE ATTACK IN KEY EXCHANGE", ARPN Journal of Engineering and Applied Sciences, ISSN 1819-6608, VOL. 7, NO. 2, FEBRUARY 2012
[59] Rikcha study: Security Aspects and Prospective Applications of RFID Systems, Federal Office for Information Security (BSI) 2004
[60] Mitko Bogdanoski, Aleksandar Risteski" Wireless Network Behavior under ICMP Ping Flood DoS Attack and Mitigation Techniques", International Journal of Communication Networks and Information Security (IJCNIS), Vol. 3, No. 1, April 2011
[61] J. Lemon, ―Resisting SYN Flood DoS Attacks with a SYN Cache, USENIX , Association Proceedings of the BSDCon 2002, Conference San Francisco, California,USA,FEB 2002.
[62] M.S. Haghighi and K. Mohamedpour, Neighbor Discovery: Security Challenges in Wireless Ad Hoc and Sensor Networks, in Trends in Telecommunications Technologies, -pp.693-714, Intech 2010 available online
[63] http://www.intechopen.com/articles//title/neighbor-discovery-security-challenges-in-wireless-ad-hoc-and-sensor-networks
[64] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, ―Truelink: A practical, countermeasure to the wormhole attack, in 14th IEEE International Conference on, Network Protocols (ICNP), November 12-15, Santa Barbara, California, USA, 2006.
[65] Jaydip Sen, Sripad Koilakoda, Arijit Ukil, "A Mechanism for Detection of Cooperative Blackhole Attack in Mobile Adhoc Networks", 2nd International Conference on Intelligent Systems mdeling and Simulation, 2011.
[66] uID Center Web Site, ―What is a ucode?―. Available: http://www.uidcenter.org/learning-about-ucode/what-is-ucode
[67] Dialog Project. Available: http://dialog.hut.fi/
[68] EPCglobal, "The EPCglobal Architecture Framework – Version 1.0, March 2005. Available: http://www.epcglobalinc.org/standards/architecture/architecture 1 0-framework-20050701.pdf.
[69] IMEI Allocation and Approval Guidelines. http://www.gsmworld.com/documents/DG06_v5.pdf
[70] CAR TO CAR Communication Consortium. Available: http://www.car-to-car.org
[71] CALM, ―The CALM handbook v1.2,September 2004.http://www.tc204wg16.de/Public/The CALM Handbookv2-060215.pdf
[72] E.163, The international public telecommunication numbering plan. Available:http://www.itu.int/rec/T-REC-E.163/en
[73] M. Tuchler, V. Schwarz, A. Huber, ―Location accuracy of an UWB localization system in a multi-path environment, IEEE International Conference on Ultra-Wideband (ICU 2005), Zurich, 5-8 Sept. 2005.
[74] Z-Wave Official Site. http://www.z-wave.com/
[75] CC2420 Single-Chip 2.4 GHz IEEE 802.15.4 Compliant and ZigBee™ Ready RF Transceiver, Datasheet. http://www.ti.com/lit/gpn/cc2420
[76] CC2530 System-on-Chip Solution for 2.4 GHz IEEE 802.15.4 / ZigBee™.Datasheet. http://www.ti.com/lit/gpn/cc2430
[77] CC2530 System-on-Chip Solution for 2.4 GHz IEEE 802.15.4 / ZigBee™.Datasheet. http://www.ti.com/lit/gpn/cc2430
[78] Texas Instruments MSP430™16-bit Ultra-Low Power MCUs. http://www.ti.com/
[79] Atmel Web Site. http://www.atmel.com/

[80] Atmel AVR Xmega Micro Controllers. http://it.mouser.com/atmel_xmega/
[81] TinyOS Alliance. (2010). TinyOS. Retrieved from http://www.tinyos.net/
[82] Dunkels, A., Gronvall, B., & Voigt, T. (2004).Contiki – A Lightweight and Flexible Operating System for Tiny Networked Sensors. Proceedings of the 29th Annual International Conference on Local Computer Networks (pp. 455-462). IEEE.
[83] Barry, R. (2010). Retrieved from http://www.freertos.org/
[84] Internet of Things - Architecture, ―State of the Art on IoT Services and Modelling, IoT-A Internal Report, IR2.1, December 2010.
[85] Liscano, R. ; Kazemi, K." Integration of component-based frameworks with sensor modeling languages for the sensor web", GLOBECOM Workshops (GC Wkshps), 2010 IEEE, Digital Object Identifier: 10.1109/GLOCOMW.2010.5700317,2010,Pages235-250,
[86] Dearle, A. ; Balasubramaniam, D. ; Lewis, J. ; Morrison, R." A Component-Based Model and Language for Wireless Sensor Network Applications", Computer Software and Applications, 2008, COMPSAC '08. 32nd Annual IEEE International, Publication Year: 2008, Page(s): 1303 – 1308
[87] Sunghyuck Hong ; Sunho Lim "Analysis of attack models via Unified Modeling Language in Wireless Sensor Networks: A survey study", Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on, Publication Year: 2010 , Page(s): 692 - 696
[88] Zelenkauskaite, A. ; Bessis, N. ; Sotiriadis, S. ;Asimakopoulou, E. " Disaster Management and Profile Modelling of IoTObjects: Conceptual Parameters for Interlinked Objects in Relation to Social Network Analysis", Intelligent Networking and Collaborative Systems (INCoS), 2012 4th International Conference on , Publication Year: 2012 , Page(s): 509 – 514
[89] Jain, S. ; Nandy, S. ; Chakraborty, G. ; Kumar, C.S. ; Ray, R. ;Shome, S.N. "Error modeling of various sensors for robotics application using Allan Variance technique", Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference on , Publication Year: 2011 , Page(s): 1 – 4
[90] Xiangyu Hu ; Songrong Qian" IoT application system with crop growth models in facility agriculture", Computer Sciences and Convergence Information Technology (ICCIT), 2011 6th International Conference on, Publication Year: 2011 , Page(s): 129 – 133
[91] Semprom Project, http://www.semprom.org/, visited October 26, 2010
[92] SENSEI D2.3 – Components for Context Modelling and Interfaces,http://www.ict-sensei.org/index.php?option=com_chronocontact&chronoformname=SENSEI_WP2_D2.3
[93] ALLOW project Website, http://www.allow-project.eu/
[94] Schnabel F, Xu L, Gorronogoitia Radzimski M, Lecue F, Ripa G, et al. D6.3.2 Advanced Specification Of Lightweight,Context-aware Process Modelling Language, http://www.soa4all.eu/pdocs/deliverables/D6.3.2.+ADVANCED+SPEC+LIGHTWEIGHT,+CONTEXT-AWARE+PROCESS+MODELLING+L.PDF
[95] SAPGravity, http://www.sapweb20.com/blog/2009/10/sap%E2%80%99s-gravityprototype-business-collaboration-using-google-wave/
[96] OGC Consortium, OpenGIS® Sensor Model Language Encoding Standard (SensorML), versión 1.0.0, http://www.opengeospatial.org/standards/sensorml
[97] Schnabel, F., Xu, L., Gorronogoitia, Y., Radzimski, M., Lecue, F., Ripa, G. et al. D6.3.2 Advanced Specification Of Lightweight, Context-aware Process Modelling Language, http://www.soa4all.eu/pdocs/deliverables/D6.3.2.+ADVANCED+SPEC+LIGHTWEIGHT,+CONTEXT-AWARE+PROCESS+MODELLING+L.PDF
[98] I. Trickovic.BPMN 2.0 - Getting started. 2008, Available: http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/50db5a00-78bc-2b10-8ba4-dfc9b66e3789?QuickLink= index&overridelayout = true (26.11.2010).
[99] Unified Service Description Language.http://www.internet-of-services.com/index.php?id=288 (2010, 09.11.2010).
[100] The Object Management Group™ (OMG™), ―Service Oriented Architecture Modelling Language (SoaML), version 1.0 - Beta 2, December 2009, http://www.omg.org/spec/SoaML/1.0/Beta2
[101] Semantic Annotations for WSDL Working Group," 2007. http://www.w3.org/2002/ws/sawsdl/
[102] W3C Semantic Sensor Networks Incubator Group (SSN-XG)." http://www.w3.org/2005/Incubator/ssn/
[103] National Institute of Standards and Technology, "IEEE 1451 " 2002. http://ieee1451.nist.gov/.
[104] National Institute of Standards and Technology, "ANSI N42.42," 2006. http://physics.nist.gov/Divisions/Div846/Gp4/ANSIN4242/xml.html.
[105] Open Geospatial Consortium Inc. OGC Reference Model 2.0; Open Geospatial Consortium Inc.: Wayland, MA, USA, 2008. (http://www.opengeospatial.org/standards/orm; Accessed: 2010, November 17)
[106] S. R. Jeffrey, G. Alonso, M. Franklin, W. Hong, J. Widom." "A pipelined framework for online cleaning of sensor data streams" ICDE, Conference, 2006

[107] S. R. Jeffrey, M. Garofalakis, M. J. Franklin.” Adaptive Cleaning for RFID Data Streams, VLDB Conference, 2006.

[108] S. R. Jeffrey, G. Alonso, M. Franklin, W. Hong, J. Widom “Declarative Support for RFID Data Cleaning”, pervasive, 2006

Chapter 3

[109] Dipashree M. Bhalerao, M. Tahir Riaz, Ole Brun Madsen, Ramjee Prasad “Scalability in IoT Architecture” Internet of Things , 3rd International Conference for Industry and Academia, IEEE-M2M, WUXI, China, ISBN: 978-1-4673-1345-2, Pages: 372 – 376, 2012

[110] Strategic Research Roadmap by European commission, 15 SEPTEMBER,2009. ••• The meaning of things ...ec.europa.eu/information_society/policy/rfid/documents/in_cerp.pdf

[111] CERP-IoT, Cluster of European Research Projects on the Internet of Things, Vision and challenges for realizing the internet of things, Edited By, Herald Sundmaeker,PatrickGuillemin,PeterFriess, Sylvie Woelffle

[112] http://wwwen.zte.com.cn/endata/magazine/zte.Technologies/2010, /no5/articles/201005/W020100510527241326851.jpg

[113] http://wwwen.zte.com.cn/endata/magazine/ztetechnologies /2010/no5/articles/201005/t20100510_184418.html

[114] http://wwwen.zte.com.cn/endata/magazine/zteCommunications 2010Year/no2/articles/201006/t20100609_186201.html

[115] [Miao Yun; Bu Yuxin “Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid “ Advances in Energy Engineering (ICAEE), 2010 International Conference on Digital Object Identifier: 10.1109/ICAEE.2010.5557611 ,Publication Year: 2010 , Page

[116] Glenford E. Mapp, FatemaShaikh, David Cottingham, Jon Crowcrof “Y-Comm: A Global Architecture for Heterogeneous Networking “Invited Paper (s): 69 – 72

[117] HaitaoPu, Jinjiao Lin, Fasheng Liu, Lizhen Cui, “An Intelligent Interaction System Architecture of the Internet of Things Based on Context”

[118] DoganYazar and Adam Dunkels. “Efficient Application Integration in IP-based Sensor Networks.” In Proceedings of ACM BuildSys 2009, the First ACM Workshop On Embedded Sensing Systems For Energy-Efficiency In Buildings, Berkeley, CA, USA, November 2009.

[119] www.bridge.eu

[120] Anggorjati, B.; C□etin, K.; Mihovska, A.; Prasad, N.R.;”RFID Added Value Sensing Capabilities: European Advances in Integrated RFID-WSN Middleware” Sensor Mesh and Ad Hoc Communications and Networks (SECON), 2010 7th Annual IEEE Communications Society Conference on Digital Object Identifier: 10.1109/SECON.2010.5508231 ,Publication Year: 2010 , Page(s): 1 – 3-ASPIRE

[121] HuanshengNing and Ziou Wang, “Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?”

[122] JiaShen, Xiangyou LU, Huafei Li, Fei XU, “Heterogeneous Multi-Layer Access and RRM for the Internet of Things “

[123] JeongGilKo, Nicolas Tsiftes, Andreas Terzis, and Adam Dunkels. “Pragmatic Low-Power Interoperability: ContikiMACvsTinyOS LPL” In Proceedings of IEEE SECON 2012, Seoul, Korea, June 2012. Best poster award.

[124] JeongGilKo, Joakim Eriksson, Nicolas Tsiftes, Stephen Dawson-Haggerty, MathildeDurvy, JP Vasseur, Andreas Terzis, Adam Dunkels, and David Culler. “Beyond Interoperability: Pushing the Performance of Sensornet IP Stacks. In Proceedings of the ACM Conference on Networked Embedded Sensor Systems,” ACM SenSys 2011, Seattle, WA, USA, November 2011.

[125] OASIS, “UDDI version 3.0.2 - UDDI spec technical committee draft,” Organization for the Advancement of Structured Information Standards (OASIS), Tech. Rep., 2004.

[126] Q. Qiu, Q. Xiong, Y. Yang, and F. Luo, “Study on ontologybased web service discovery,” in IEEE Internationl Conference on Computer Supported Cooperative Work in Design,vol. 11, 2007, pp. 641–645.

[127] S. Li, C. Xu, Z. Wu, Y. Pan, and X. Li, “ABSDM: Agentbased service discovery mechanism in internet,” in Proceed ings of ICCS 2004, ser. LNCS 3036, 2004, pp. 441–444.

[128] S. Degwekar, H. Lam, and S. Y. W. Su, “Constraint-based brokering (CBB) for publishing and discovery of web services,” in LLC, 2007.

[129] A. Kassim, B. Esfandiari, S. Majumdar, and L. Serghi, “A flexible hybrid architecture for management of distributed web service registries,” in Communication Networks and Services Research (CNSR), vol. 5, 2007.

[130] Y. Li, S. Su, and F. Yang, “A Peer-to-Peer approach to semantic web service discovery,” in Proceedings of ICCS2006, ser. LNCS 3994, vol. 4, 2006, pp. 73–80.

[131] Ali Modirkhazeni, NorafidaIthnin , Othman Ibrahim , "Secure Multipath Routing Protocols in Wireless Sensor Networks: A Security Survey Analysis "

[132] Tomás Sánchez López, Damith C. Ranasinghe, Mark Harrison, Duncan Mcfarlane "Adding sense to the Internet of Things "Personal and Ubiquitous Computing , Volume 16 Issue 3, March 2012, Publisher: Springer

[133] Curran, K. ; Parr, G. "The use of dynamically reconfigurable protocol stacks for streaming multimedia to mobile devices", Communication Systems, 2002. ICCS 2002. The 8th International Conference on,, Volume: 2, Digital Object Identifier: 10.1109/ICCS.2002.1183273, Publication Year: 2002 , Page(s): 947 - 951 vol.2

[134] Chunjie Zhou ; Hui Chen ; Naixue Xiong ; Vasilakos, A.V. "Function Block Design for the Reconfigurable Protocol Stack in Networked Control Systems", Communications (ICC), 2011 IEEE International Conference on, Digital Object Identifier: 10.1109/icc.2011.5962822 , Publication Year: 2011 , Page(s): 1 - 5

[135] Crane, S. ; Dulay, N." A configurable protocol architecture for CORBA environments" Autonomous Decentralized Systems, 1997. Proceedings. ISADS 97., Third International Symposium on, Digital Object Identifier: 10.1109/ISADS.1997.590621, Publication Year: 1997 , Page(s): 187 - 194

[136] Gazis, V. ; Alonistioti, N. ; Merakos, L." Discovering Feasible Protocol Stack Combinations in Beyond 3G Systems: Information Model, Search Algorithms and Performance", Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on, Digital Object Identifier: 10.1109/PIMRC.2007.4394609 Publication Year: 2007 , Page(s): 1 - 6

[137] Darren R. Law " scalable means more than more: a unifying definition of simulation scalability".Proceedings of the 1998 Winter Simulation Conference D.J. Medeiros, E.F. Watson, J.S. Carson and M.S. Manivannan, eds.

[138] Leticia Duboc, Prof. David S. Rosenblum, Dr. Tony Wicks " A Framework for Modelling and Analysis of Software Systems Scalability"ESEC-FSE '07: Proceedings of the the 6th joint meeting of the European software engineering conference and the ACM SIGSOFT symposium on The foundations of software engineering, September 2007

[139] www.Arduino.cc\

Chapter 4

[140] Adam Dunkels. Full TCP/IP for 8 Bit Architectures. In Proceedings of the First ACM/Usenix International Conference on Mobile Systems, Applications and Services (MobiSys 2003), San Francisco, May 2003

[141] Rong Chai; Wei-Guang Zhou; Qian-Bin Chen; Lun Tang "A survey on vertical handoff decision for heterogeneous wireless networks " Information, Computing and elecommunication, 2009. YC-ICT '09. IEEE Youth Conference on Digital Object Identifier:, 10.1109/YCICT.2009.5382368 Publication Year: 2009 , Page(s): 279 – 282

[142] Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi"

[143] Zacharias, S. ; Newe, T. ; O'Keeffe, S. ; Lewis, E. ITS Telecommunications (ITST), 2012 12th International Conference on, Digital Object Identifier: 10.1109/ITST.2012.6425289 ,Publication Year: 2012 , Page(s): 785 – 790

[144] Garroppo, Rosario G "Experimental assessment of the coexistence of Wi-Fi, ZigBee, and Bluetooth devices" ,World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a, 20-24 June 2011,Page(s)**:** 1 - 9

[145] M. Howlader, C.J. Kiger and P.D. Ewing "Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Facility Environment" Division of Fuel, Engineering and Radiological Research, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, July 2007

[146] Axel Sikora, Voicu F. Groza "Coexistence of IEEE802.15.4 with other Systems in the 2.4 GHz-ISM-Band", in Proc. IEEE Instrumentation & Measurement Technology Conference, Ottawa, May 2005, pp.1786-1791.

[147] Texas Instruments Product Bulletin (2003), Wireless performance optimization solutions:Bluetooth and 802.11 co-existence. http://focus.ti.com/pdfs/vf/wireless/co-existencebulletin.pdf

[148] Coexistence measurements and analysis of IEEE 802.15.4 with Wi-Fi and bluetooth for vehicle networks

[149] K. Shuaib, M. Boulmalf, F. Sallabi, and A. Lakas, "Co-existence of Zigbee and WLAN: A performance study," in Proc. IEEE/IFIP Int. Conf. Wireless & Optical Communications Networks, Bangalore, India, April,2006

[150] K. Shuaib, M. Boulmalf, F. Sallabi and A. Lakas "Co-existence of Zigbee and WLAN, A Performance Study"

[151] P. S. Neelakanta and H. Dighe, "Robust factory wireless communications: A performance appraisal of the Bluetooth and the ZigBee collocated on an industrial floor," in *Proc. IEEE Int. Conf. Ind. Electron.* (IECON'03), Roanoke, VA, Nov. 2003, pp. 2381-2386.

[152] Budhwani, S. ; Sarkar, M. ; Nagaraj, S."A MAC Layer Protocol for Sensor Networks Using Directional Antennas", Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010 IEEE International Conference on, Digital Object Identifier: 10.1109/SUTC.2010.11 , Publication Year: 2010 , Page(s): 261 – 267

[153] https://developer.bluetooth.org/TechnologyOverview /Pages/OverviewOfOperations.aspx

[154] https://docs.zigbee.org/zigbee-docs/dcn/07-5219.PDF

[155] Jordan Douglas Guffey "OFDM Physical Layer Implementation for the Kansas University Agile Radio", ITTC-FY2008-TR-31620-06, February 2008

[156] Sirigir, V.K. ; Alzoubi, K. ; Saab, D.G. ; Kocan, F. ;Tabib-Azar, M. "Ultra-low-Power Ultra-fast Hybrid CNEMS-CMOSFPGA" Field Programmable Logic and Applications (FPL), 2010 International Conference on, Digital Object Identifier: 10.1109/FPL.2010.79 , Publication Year: 2010 , Page(s): 368 - 373

[157] Henry, M.B. ; Nazhandali, L." Design techniques for functional-unit power gating inthe Ultra-Low-Voltage region" Design Automation Conference (ASP-DAC), 2012 17th Asia and South Pacific, Digital Object Identifier: 10.1109/ASPDAC.2012.6165029 , Publication Year: 2012 , Page(s): 609 - 614

[158] ECMA-368 standard, "High rate ultra wideband PHY and MAC standard", 2nd Edition, December 2007

[159] https://docs.zigbee.org/zigbee-docs/dcn/07-5219.PDF

[160] A. Eyadeh, "Frame Synchronization Symbols for an OFDM System," International Journal of Communications, Issue 1, vol. 2, 2008.

[161] M. I. Rahman, S. Sekhar Das, and F. H. P. Fitzek, "OFDM Based WLAN Systems," Center for TeleInFrastruktur (CTIF), Aalborg University, Tech. Rep., 2005

[162] digital equipment corporation maunard, Massachusetts DECnet, " DIGITAL Network Architecture , (Phase IV)"

[163] Zheng, J. ; Jamalipour, A. "Network Architectures and Protocol Stack", Wireless Sensor Networks:A Networking Perspective, Digital Object Identifier: 10.1002/9780470443521.ch2 , Page(s): 19 - 33 , Copyright Year: 2009

[164] Glenford E. Mapp, FatemaShaikh, David Cottingham, Jon Crowcrof "Y-Comm: A Global Architecture for Heterogeneous Networking "Invited Paper ,WICON '07: Proceedings of the 3rd international conference on Wireless internet , October 2007

[165] Betzler, August ; Gomez, Carles ; Demirkol, I. ; Paradells, J." Should we use the default protocol settings for networks" Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2012 10th International Symposium on,, Publication Year: 2012 , Page(s): 305 – 310

[166] Jin Mitsugi, Shigeru Yonemura, Hisakazu Hada, Tatsuya Inaba "Bridging UPnP and ZigBee with CoAP: protocol and its performance evaluation,", December 2011, IoTSP '11: Proceedings of the workshop on Internet of Things and Service Platforms, ACM

[167] Atiquzzaman, M. ; Reaz, A.S. "Survey and classification of transport layer mobility management schemes ",Personal, Indoor and Mobile Radio Communications, 2005. PIMRC 2005. IEEE 16th International Symposium on, Volume: 4, Digital Object Identifier: 10.1109/PIMRC.2005.1651818 , Publication Year: 2005 , Page(s): 2109 - 2115 Vol. 4

[168] Oscar Garcia-Morchon, Sye Loong Keoh, Sandeep Kumar, Pedro Moreno-Sanchez, Francisco Vidal-Meca, Jan Henrik Ziegeldorf ," Securing the IP-based internet of things with HIP and DTLs", WiSec '13: Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, April 2013, ACM

[169] K.D. Korte, I. Tumar, and J. Sch¨onw¨alder, Evaluation of 6lowpan Implementations In 4th IEEE International Workshop on Practical Issues in Building Sensor Network Applications (SenseApp 2009). IEEE, October 2009

[170] Ju, P. ; Song, W. ; Zhou, D. "Survey on cooperative medium access control protocols", Communications, IET, Volume: 7 , Issue: 9 , Digital Object Identifier: 10.1109/COMST.2004.5342231 , , Publication Year: 2004 , Page(s): 2 – 1

[171] Khan, R. ; Karl, H. "MAC Protocols for Cooperative Diversity in Wireless LANs and Wireless Sensor Networks " , Communications Surveys & Tutorials, IEEE , Volume: PP , Issue: 99 , Digital Object Identifier: 10.1109/SURV.2013.042313.00067 , Publication Year: 2013 , Page(s): 1 – 18

[172] Lakshmisudha, K. ; Arun, C. , "Research on power optimization in physical and MAClayer of wireless sensor networks — A survey", Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on, Digital Object Identifier: 10.1109/ISSP.2013.6526915 , Publication Year: 2013 , Page(s): 262 – 267

Chapter 5

[173] http://en.wikipedia.org/wiki/Mobile_ad_hoc_network.

[174] Jaydip Sen, Sripad Koilakoda, Arijit Ukil, "A Mechanism for Detection of Cooperative Blackhole Attack in Mobile Adhoc Networks", 2nd International Conference on Intelligent Systems Modeling and Simulation, 2011.

[175] Vishnu K, Amos J Paul, "Detection and Removal of Cooperative Black/Grey hole attack in Mobile ADHOC Networks", ©2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 22, 2010 IEEE.

[176] Bosworth Seymour, Kabay M.E., Whyne Eric, " Computer security handbook volume I & I", 5th edition, John Wilsons publication

[177] Piyush Agrawal, R. K. Ghosh, "Cooperative Black and Grey Hole Attacks in Mobile Ad Hoc Networks".

[178] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU, "An Adaptive Approach to Detecting Black and Grey Hole Attacks in Ad Hoc Network", 2010 24th IEEE International Conference on Advanced Information Networking and Applications.

[179] Devu Manikantan Shila, Yu Cheng and Tricha Anjali, "Channel-Aware Detection of Grey Hole Attacks in Wireless Mesh Networks".

[180] Onkar V.Chandure, Vishal Vig, Nagesh Chand V.T.Gaikwad, "Detection & Prevention of Grey Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol", International International Journal of Computer Applications (0975 – 8887) Volume 41– No.5, March 2012.

[181] Acknowledgement Based Scheme in MANET", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010

[182] Aishwarya Sagar Anand Ukey, Meenu Chawla, "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010

[183] Marjan Kuchaki Rafsanjani, Zahra Zahed Anvari, Shahla Ghasemi, "Methods of Preventing and Detecting Black/Grey Hole Attacks on AODV-based MANET", IJCA Special Issue on "Network Security and Cryptography" NSC, 2011.

[184] Himadri Nath Saha , Prof. (Dr.) Debika Bhattacharyya , Prof.(Dr.) P. K. Banerjee, "A Distributed Administration Based Approach for Detecting and Preventing Attacks on Mobile Ad Hoc Networks", International Journal of Scientific & Engineering Research Volume 2, Issue 3, March-2011.

[185] DHAMANDE C.S. AND DESHMUKH H.R., "A COMPETENT WAY TO DIMINISH THE BRUNT OF GREY HOLE ATTACK IN MANET", International Journal of Wireless Communication ISSN: 2231-3559 & E-ISSN: 2231-3567, Volume 2, Issue 1, 2012, pp.-29-34.

[186] http://www.faqs.org/rfcs/rfc3561.html

Chapter 6

[187] http://data.worldbank.org/topic/agriculture-and-rural-develo...

[188] Oner, M.A.; Basoglu, N.; Ture, E, "Technology and rural development: assessing technology needs of the Southeastern Anatolia Project in Turkey" Management of Engineering and Technology, 1999. Technology and Innovation Management. PICMET '99. Portland International Conference on Digital Object Identifier: 10.1109/PICMET.1999.808492

[189] The 11th Strategic Workshop SW'09 in Rebild, Denmark 2009, "on Wireless Innovation for InterDynamicTecHnology."

[190] Raj Ashar, Sheri Lewis, David Blazes, J.P.Chretein "Applying information and communication technologies to collect health data from remote settings: A systematic assessment of current technologies" journal of biomedical informatics.

[191] Y. Okumura, E. Ohmori, T. Kawano, and K.Fukuda, "Field strength and its variability in VHFand UHF land-mobile service," Rev. Elec. Comm.Lab.,vol. 16,No. 9-10,pp. 825-873, 1968.

[192] Okumura-Hata propagation prediction model for UHF range, in the "Prediction methods for the terrestrial land mobile service in the VHF and UHF bands"// ITU-R Recommendation P. 529-2.Geneva: ITU, pp. 5-7, 1995.

[193] Rural Development in the European Union-statistical and economic information –report 2007",OOPEC 2007.
[194] The Eu Rural Development policy 2007 -2013. Luuxembiurg OOPEC, 2006.

Chapter 7

[195] http://techon.nikkeibp.co.jp/english/NEWS_EN/20090326/167757/
[196] H. Chinthaka N. Premachandra, Tomohiro Yendo, Mehrdad Panahpour Tehrani, Takaya Yamazato, Hiraku Okada, Toshiaki Fujii, and Masayuki Tanimoto "High-speed-camera Image Processing Based LED Traffic Light Detection for Road-to-vehicle Visible Light Communication" 2010 IEEE Intelligent Vehicles Symposium University of California, San Diego, CA, USA, June 21-24, 2010
[197] TANAKA Y., HARUYAMA S., NAKAGAWA M.: 'Indoor visible light data transmission system utilizing white LED lights', IEICE Trans. Communes., 2003, E86-B, (8), pp. 2440–2454
[198] Rajagopal, S.; Roberts, R.D.; Sang-Kyu Lim "IEEE 802.15.7 visible light communication: modulation schemes and dimming support" Communications Magazine, IEEE Volume: 50 , Issue: 3 ,Topic(s): Communication, Networking & Broadcasting ,Publication Year: 2012 , Page(s): 72 – 82

Appendix

Appendix A: List of Publications

Sr.No	Paper Title	Status	Conference /Journal
1	An Internet of Things Generic Reference Architecture	Accepted	NewWorldPublishers, IoT journal
2	IoT Heterogeneous Interoperable Network Architecture Design using ZB-Fi Access Point	Accepted	NewWorldPublishers, IoT journal
3	Scalability in IoT Architecture	Published	M2M, WUXI, China
4	On New Global Catastrophic ICT Model	published	ICACT, IEEE, South Korea
5	On the Use of the Universal Okumura-Hata Model for Defining Different ICT Areas	Published	IMTC Pakistan, Springer
6	Rural, Poor and Catastrophic ICT Area Standardization and Modelling	Published	WPMC,IEEE, Taiwan

Appendix B: Short CV

Dipashree Milind Bhalerao received her B.E.degree in 1991 from Pune university, Maharashtra, India. She rerecived her Masters degree in 2008 from Bharati Vidyapeeth Deemed University, Pune. She has recently obtained her PhD degree from CTIF, Aalborg University, Denmark under the guidance of Prof.Ramjee Prasad. Her research Interests include *IoT, Wireless Communication (VLC), Network Architecture, Mechatronics, Green energy, and security*.

She was working as computer hardware engineer for one year from Aug. 1991 to Aug. 1992 in Fortune Computers Pvt.Ltd, Pune India. She was working as a R&D engineering at Inventa Electronic Pvt.Ltd from 1992 to 1995, at Pune. She started own computer training center *(CDAC -Pace Bureau) at Mundhawa in 1995 till 2004.*

She is teaching to UG as well as PG from 2001. She is presently working as Professor in Sinhgad College of Engineering, Vadgaon, Maharashtra, India.

Appendix C: List of Figures

Appendix D: List of Abbreviations

IoT	Internet of Things
HI	Heterogeneous Interoperability
RPC	Rural, Poor and Catastrophic Area
RFID	Radio Frequency Identification
EPC	Electronic Product Code
SOA	Service Oriented Architecture
WoB	Web of Things
ROA	Resource Oriented Architecture
HTML	Hypertext mark-up language
PHP	Hypertext Pre-processor
NFC	Near Field Communication
ONS	object naming server
OIS	object information service
WSN	Wireless Sensor network
6LoWPAN	Ipv6 over Low power Wireless Personal Area Networks
CERP-IoT	Cluster of European Projects on the IoT
WHO	World Health Organization
SToP	Stop tampering of products
CuteLoop	Customer in the Loop: Using Networked Devices enabled Intelligence for Proactive Customers Integration as Drivers of Integrated Enterprise
STOLPAN	Store Logistics and Payment with NFC
SMART	Intelligent Integration of Supply Chain Processes and Consumer Services based on Unique Product Identification in a Networked Business Environment
GRIFS	Global RFID Interoperability Forum for Standards
BRIDGE	Building Radio frequency Identification solutions for the Global Environment
ASPIRE	Advanced Sensors and light weight Programmable middleware for Innovative RFID Enterprise applications
HYDRA	Heterogeneous physical devices in a distributed architecture
UML	Unified Modelling Language
PDA	personal digital assistant

Wi-Fi	Wireless Fidelity
Wi-MAX	Worldwide Interoperability for Microwave Access
UMT	Universal Mobile Telecommunication
ATM	Asynchronous Transfer Mode (ATM
MPLS	Multiprotocol Label Switching
CPU	Central Processing Unit
NS	Network Simulator
BCD	Binary coded decimal
VHO	Vertical Handoff
HHO	Horizontal Handoff
AP	Access point
BS	Base station
WLAN	Wireless Local area Network
WWAN	Wireless Wide Area Network
CAPEX	Capital Expenditures
OPEX	Operating Expenditures
GENI	Global Environment for Network Innovations
MAC	Media Access Control
XML	Extensible Mark-up Language
GPS	Global Positioning System
SNR	Signal to noise ratio
BER	Bit Error rate
MANET	Mobile Ad-Hoc Network
AODV	On-Demand Distance Vector
CTS	Clear to Send
RTS	Request to send
OS	Operating System
QoS	Quality of Service
PAN	Personal Area Network
LAN	Local Area Network
WAN	Wide Area Network
VAN	Virtual Area Network
VPN	Virtual Private Network

VANET	Vehicular Ad Hoc Networks
ZRP	Zone Routing Protocol
RREQ	Route request
RREPS	Route replies
RERR	Route Errors
TTL	Time to Live
CGH	Co-operative Grey Hole
RN	Reliable Node
CBH	Co-operative Black Hole
ICT	Information and Communication Technology
UDP	User Datagram Protocol
CBR	Constant Bit Rate
DoS	Denial of service attack
IT	Information Technology
ISO	International Organization for Standardization
ITU	International Telecommunication Union
IETF	Internet Engineering Task Force